... بلاک (سیکٹر) اسلام آباد

ابرا چوہدا

Group

محبت کی یوں ادا کی صداقت

مجھے بے مروت بھی تو حسن والے ۔ ہمیں دل لگانے کی کوشش نہ کرنا

ہنسی آتی ہے آج ہر جا دکھاں پہ ۔ اسے ہمدم ہر دم

میرے دل کے زخموں کو نیند آگئی ہے انہیں تم جگانے کی کوشش نہ کرنا

حقیقت تو ہے آپ کا منزل نا کر ۔ ادھر کھو گئے حسن کی جو یاد ...

زندگی نے تصور میں تم ڈوب جاؤ ۔ لگا کر ملانے کی کوشش ...

مرے صورت کیا حسن والے

ذرا لگا کر جانا آنکھوں میں تم یہ آنسو ۔ ایسی دنیا کو ... حسن ...

ہمارا نام رہے ہمیں زندگی بھر ۔ مگر اس بستی کی کوشش نہ کرنا

ستم کر ستم کی شکایت نہ ہم کر سکے ہیں نہ ہم کر سکیں گے

میرے آنسو تم مرا ساتھ دینا ۔ ابھی کچھ ستانے کی کوشش نہ کرنا

سمجھ لے گے محفل میں ہم حال دل ۔ مگر دل کی جاں کے ہیں پروانہ جیسی

خدا کی قسم جان دے دیں گے ہم پر ابھی ہم کو آزمانے کی کوشش نہ کرنا

Group Theory

ATTESTED

Magistrate 1st. Class
LAHORE.

Set

A set is a collection of distinct and and distinguishable objects of any sort, having some proper ties in common.

A set is finite or infinite according to number of its elements is finite or infinite.

Singleton Set

A set having single element is called as singleton set e.g $\{a\}, \{0\}$

Null Set or Void set or Empty Set

A set having no element is called an empty set and is denoted by ϕ i.e.

$$\phi = \{ x : x \neq x \}$$

Sub Set

If every element of a set A is is a member of B, then A is called subset of B or A is said to be contained in B and noted by

$$A \subseteq B$$

i.e A is eneluded or contained in B or B contain A or B is super set of A

Proper Sub Set

A set A is proper subset of a set B, if A is sub-set of B but not the same as B. It is denoted by

$$A \subset B$$

OR

A set A is said to be the proper subset of B, if every element of A is an element of B and there is at least one element of B which is not the element of A i.e $A \neq B$

Note A sub-set of set A other than a void set

and itself is called proper subset of A.

Equal Sets

Two sets A and B are said to be equal if they have same elements, i.e if

$$A \subseteq B \text{ and } B \subseteq A$$

Equivalent Sets OR Equipotent Sets

Two sets A & B are said to be equivalent if the number of elements of A is equal to the number of elements of B. Equivalence of A & B is denoted by

$$A \sim B$$

Power Set

If S is any set, then the set of all the subsets of S is called the power set of S and is denoted by P(S) i.e

$$P(S) = \{A : A \subseteq S\}$$

If there are n elements in S, then there are 2^n elements in P(S).

Union of Sets

The union of two sets A & B is the set $A \cup B$ (A cup B) consisting of all those elements which are either in A or in B or in both. i.e

$$A \cup B = \{x / x \in A \text{ or } x \in B\}$$

Intersection of Sets

The intersection of two set $A \cap B$ (A cap B) is the set $A \cap B$ consisting of all those elements which are common to both A and B i.e.

$$A \cap B = \{x / x \in A \text{ and } x \in B\}$$

Family of Sets

If I be a non-empty set, then a collection of sets such that to each member of I, there corresponds a member of the collection of sets, is called indexed family of sets and I is called indexing set

Indexed family of sets $A_\alpha, \alpha \in I$ is denoted by $\{A_\alpha : \alpha \in I\}$ or $A_\alpha : \alpha \in I$

The union of an arbitrary family of sets $\{A_\alpha : \alpha \in I\}$ is denoted by

$\bigcup_{\alpha \in I} A_\alpha$ or $\bigcup \{A_\alpha : \alpha \in I\}$ and is defined as

$$\bigcup_{\alpha \in I} A_\alpha = \{x / x \in A_\alpha \text{ for at least one } \alpha \in I\}$$

Similarly arbitrary intersection of an indexed family $\{A_\alpha : \alpha \in I\}$ is given by

$$\bigcap_{\alpha \in I} A_\alpha = \{x / x \in A_\alpha \ \forall \alpha \in I\} \qquad (\forall \Rightarrow \text{for every})$$

Universal Set

All the sets under consideration are assumed to the subsets of some fixed set called as universal set and is denoted by U.

Complement of a Set

The complement of a set A is denoted by A' and is defined as the set of all members of the universal set U, which are not members of A i.e

$$A' = \{x / x \in U \text{ and } x \notin A\}$$

Note $A \cup A' = U$; $U' = \phi$; $\phi' = U$ $A \cap A' = \phi$

and $(A')' = A$.

Difference of Sets

If A & B are two sets, then the set of all those elements which belong to A but not to B is said to be the difference of sets A & B and is denoted by $A - B$ i.e.

$$A - B = \{x / x \in A \text{ and } x \notin B\}$$

If B is subset of A, then $A - B$ is called the complement of B w.r.t A

Symmetric Difference of two Sets

The symmetric difference of A & B denoted by $A \Delta B$ is defined as

$$A \Delta B = (A - B) \cup (B - A)$$

Commutative Laws

(i) $A \cup B = B \cup A$ (ii) $A \cap B = B \cap A$.

Proof (i) Let $x \in A \cup B$

$\Rightarrow x \in A$ or $x \in B$

$\Rightarrow x \in B$ or $x \in A$

$\Rightarrow x \in B \cup A$

$\Rightarrow A \cup B \subseteq B \cup A$ ——→ (1)

Similarly $B \cup A \subseteq A \cup B$ ——→ (2)

By (1) and (2)

$A \cup B = B \cup A$.

Associative Laws

(i) $A \cup (B \cup C) = (A \cup B) \cup C$

(ii) $A \cap (B \cap C) = (A \cap B) \cap C$

Proof (i) Let $x \in A \cup (B \cup C)$

$\Rightarrow x \in A$ or $x \in (B \cup C)$

$\Rightarrow x \in A$ or $x \in B$ or $x \in C$

$\Rightarrow x \in A$ or $x \in (B \cup C$

$\Rightarrow x \in (A \cup B)$ or $x \in C$

$\Rightarrow x \in (A \cup B) \cup C$

$\Rightarrow A \cup (B \cup C) \subseteq (A \cup B) \cup C \longrightarrow ①$

Similarly $(A \cup B) \cup C \subseteq A \cup (B \cup C) \longrightarrow ②$

By ① & ②

$$A \cup (B \cup C) = (A \cup B) \cup C$$

Similarly (ii) can be proved.

Distributive laws

(i) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(ii) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

De Morgan Laws

If A & B are subsets of universal set U. then

(i) $(A \cup B)' = A' \cap B'$

(ii) $(A \cap B)' = A' \cup B'$

If $A \cap X = A \cap Y$ and $A \cup X = A \cup Y \Rightarrow X = Y$

Remark If a set A has n elements, then we write $|A| = n$ and for two sets A & B

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Cartesian Product

Given two sets A & B, the Cartesian product $A \times B$ is defined as the set of ordered pairs of the form (a, b) where $a \in A$ and $b \in B$ i.e

$A \times B = \{(a, b) \mid a \in A, b \in B\}$ $A \times B$ is read as A Cross B.

$$A \times B \neq B \times A$$

If either A or B is null set, then $A \times B = \phi$

If the set A has m elements and B has n elements, then $A \times B$ and $B \times A$ has mn elements (ordered pairs).

The product of n sets $A_1, A_2, \ldots A_n$ is the set of ordered n-tuples $(a_1, a_2, \ldots, a_n)$ where $a_1 \in A_1, a_2 \in A_2, \ldots a_n \in A_n$ and is defined as

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2 \ldots, a_n) : a_1 \in A_1, \ldots a_n \in A_n\}$$

Mappings or Function

Binary Relation

Let X and Y be two non-empty sets. Then any subsets of $X \times Y$ is called a binary relation of X to Y. A relation is also called a correspondence.

Thus if $(x, y) \in R$, then we write xRy and say x has a relation R to y.

Binary Relation on a Set

Binary relation on a the set S is a subset of $S \times S$.

If there are m elements in X and n in Y then there will be mn elements in $A \times B$ and so there will be different 2^{mn} relations from X to Y.

Domain and Range of a relation

The domain of relation R from X to Y denoted by Dom R is the set of first co-ordinates of all the ordered pairs in R and range of R denoted by Ran R is the set of all 2nd co-ordinates of all the ordered pairs in R. Thus

$$\text{Dom } R = \{x : (x, y) \in R \text{ for some } y \in Y\}$$

$$\text{Ran } R = \{y : (x, y) \in R \text{ for some } x \in X\}$$

Identity or Diagonal Relation

A relation R on a set A is known as identity relation or diagonal relation iff $xRy \Rightarrow x = y \quad \forall x, y \in A$

$\Delta = \{(x, x) / x \in A\}$

Note If A is a set, the set $\{(x, x) / x \in A\}$ is called the diagonal of $A \times A$.

Composite Relation

If R be a relation from A to B and S is a relation from B to C, then the composite relation from A to C is denoted by SoR and is defined as the set of all ordered pairs $(x, z) \in SoR$ iff $\exists$ a $y \in B$ s.t that xRy and ySz. In other words

$$SoR \subseteq Dom(R) \times Ran(S)$$

Universal Relation

If A is any set and R is the set $A \times A$, then R is said to be the universal relation on A.

Inverse Relation

If R is a relation on a set A to another set B, then the inverse relation of R denoted by R^{-1}, is defined as

$$R^{-1} = \{(y, x) : (x, y) \in R\}$$

Types of Relations

A relation R on a set A is

(i) Reflexive, if $(a, a) \in R$ for every $a \in A$ i.e if each member of A is R-related to itself i.e $aRa \quad \forall a \in A$

(ii) Symmetric if $aRb \Rightarrow bRa$; $a, b \in A$ i.e $(a, b) \in R \Rightarrow (b, a) \in R$

evidently a relation R on A is symmetric if $R = R^{-1}$

(iii) Anti-symmetric if $aRb \wedge bRa \Rightarrow a = b$ i.e $(a, b) \in R$ and $(b, a) \in R \Rightarrow a = b \quad a, b \in A$

(iii) Transitive if $aRb \wedge bRc \Rightarrow aRc$

e.g. if xRy = x divides y in $\mathbb{Z}$ is anti-symmetric since x divides y and y divides $x \Rightarrow x = y$ i.e. xRy and $yRx \Rightarrow x = y$

Illustrations

- The relation "is equal to" in any set is reflexive, symmetric and transitive.
- The relation "Is divisor of" is reflexive, not symmetric, anti-symmetric and transitive.
- The relation "Contained in" in the power set of a set is reflexive, anti-symmetric and transitive but not symmetric.
- In respect of the set of all analytic functions of a complex variable the relation "Is a continuation of" is reflexive, anti-symmetric and transitive.
- The $a \parallel b$ of parallelism in the set of all straight lines is symmetric, transitive and reflexive.
- The relation "is perpendicular" in the set of all straight lines is symmetric but neither reflexive not transitive.
- The relation "Loves" in the set of all human being is devoid of reflexivity, symmetry as well as transitivity. It is not even anti-symmetric.

Equivalence Relation

A relation R on a set X is said to be equivalence relation if it is at the same time reflexive, symmetric and transitive.

Equivalence set (or class)

Let R be an equivalence relation on a non-empty set S and let $x \in S$; then the elements satisfying yRx constitute a subset of S, known as [illegible] set of x w.r.t R i.e.

cl(x) or

C_x or S_x or $\bar{x}$ or $[x] = \{y : y \in S \text{ and } y R x\}$

The equivalence set of has the following properties

(i) If $z \in [x]$ then $[z] = [x]$

(iii) $[x] = [z]$ iff $x R z$

(iii) If $[x] \cap [z] \neq \phi$, then $[x] = [z]$ i.e two equivalence classes are either disjoint or equal.

Examples

- The ordinary relation of equality of two elements in a set S is an equivalence relation on S
- The relation of parallelism in the set all lines in a plane is an equivalence relation
- Let n be a fixed +ve integer. For any two integers a, b, define $a \equiv b \pmod n$ if and only if n divides a−b. It can be varified

(i) $a \equiv a \pmod n$ (ii) $a \equiv b \pmod n \Rightarrow b \equiv a \pmod n$

(iii) $a \equiv b \pmod n, b \equiv c \pmod n \Rightarrow a \equiv c \pmod n$

Thus the relation $\equiv$ on Z is an equivalence relation This relation is known as the relation of Congruence modulo n

Partial order / ordering Relation

A relation R on a set X is said to be partial ordering / order relation if it is at the same time reflexive, anti-symmetric and transitive. It is usually denoted by $\preceq$

Remark If R is a relation on set A and a R b, then a, b are called comparable otherwise incomparable relatively to the relation R

Total ~~order~~ Relation

A relation R on a set S is said to be total if any two elements of S are comparable relatively to R

Total order Relation

Let R be a partial order relation on a set S. Then R is called total order relation if any two different elements of S are Comparable in respect of the partial ordering relation R

Chain

A set provided with a total order relation is called a chain

Example

For any $a, b \in N$, the set of natural numbers define $a \leq b$ if and only if a divides b. Then for any three natural no a, b, c

(i) Since $a = 1a \Rightarrow a$ divides a, so $a \leq a$

(ii) $a \leq b$, $b \leq a \Rightarrow a$ divides b and b divides a

$\Rightarrow a = b$

$\Rightarrow \leq$ is anti-symmetric

(iii) $a \leq b$, $b \leq c \Rightarrow a/b$ and b/c

$\Rightarrow a/c \Rightarrow a \leq c$

$\Rightarrow \leq$ is transitive

Hence relation $\leq$ is a partial ordering on N.

Partition of a Set

A partion of a set is a family of subsets of the set such that their union is the set itself, and any two subsets are disjoint i.e subsets are mutually exclusive or disjoint.

Theorem Let R be an equivalence relation on a set X. Then for any $a, b \in X$

(i) $a \in Cl(a) = [a] = \bar{a} = Ca$

(ii) Either $Ca \cap Cb = \phi$ or $Ca = Cb$ (i.e any two equivalence classes are either disjoint or equal)

Proof

(i) by defination

$Cl(a) = Ca = \{b \in X \mid b R a\}$

Since R is reflexive

$\therefore aRa \Rightarrow a \in Ca = Cl(a)$

(ii) Let $Ca \cap Cb \neq \phi \Rightarrow \exists x \in Ca \cap Cb$

$\Rightarrow xRa$ and xRb

$\Rightarrow xRa$ and xRb

$\Rightarrow aRx$ and xRb (by Symmetry of R)

$\Rightarrow aRb$ (by transitivity of R) $\longrightarrow$ ①

Let $y \in Cb \Rightarrow yRb$

But aRb by ①

$\Rightarrow bRa$ (by symmetry of R)

Hence $yRb, bRa \Rightarrow yRa \Rightarrow y \in Ca$

$\longrightarrow$ Ⓐ

Thus $Cb \subseteq Ca$

Similarly interchanging the role of a & b we get

$Ca \subseteq Cb$ $\longrightarrow$ Ⓑ

By Ⓐ & Ⓑ

$Ca = Cb$

(iii) X is the union of the set of equivalence classes

$F = \{Ca \mid a \in X\}$

Proof Set $E = \bigcup_{a \in X} Ca$

Clearly $E \subseteq X$

Since for each $a \in X$, $a \in Ca \Rightarrow a \in E$ and we get $X \subseteq E$

Hence $X = E = \bigcup_{a \in X} Ca$

Remark From this theorem we have seen that an equivalence relation decomposes X into disjoint equivalence classes. Thus $F = \{Ca \mid a \in X\}$ is a partition of X. Hence each equivalence relation on a set X determines a partition of X. We prove the converse.

Theorem Any partition of a set X into a set of mutually disjoint classes give rise to an equivalence relation. Correspondig partition of X coincides given Partition of R

Let $F = \{S_\alpha\}_{\alpha \in I}$ be a partition of X. Then there exists an equivalence relation on X, such that F is the set of all equivalence classes under that relation

Proof For any $a, b \in X$, define aRb iff a, b are in same S_α. Then for a, b, c in X we have.

(i) Reflexivity:

$\because$ by defination $X = \bigcup_{\alpha \in I} S_\alpha$

$\Rightarrow a \in S_\alpha$ for some α

$\Rightarrow aRa$

(ii) Symmetry:- $aRb \Rightarrow a, b \in S_\alpha$ for some $\alpha \in I$

$\Rightarrow b, a \in S_\alpha$ " "

$\Rightarrow bRa$

(iii) Transitivity: $aRb, bRc \Rightarrow \exists\ \alpha, \beta \in I$ such that $a, b \in S_\alpha$ and $b, c \in S_\beta$

if $\alpha \neq \beta$ then by defination $S_\alpha \cap S_\beta = \phi$

However $b \in S_\alpha \cap S_\beta$; so $\alpha = \beta$ and

Consequently $a, c \in S_\alpha$ and aRc

Hence R is an equivalence relation on X

Consider any S_α and $a \in S_\alpha$

Now $C_a = \{b \in X \mid bRa\}$

Since bRa if a, b are in the same member of F, as $a \in S_\alpha$ we set $b \in S_\alpha$. Hence

$C_a = S_\alpha$

So that each S_α is an equivalence class

Conversly since given any $b \in X$, $b \in S_\beta$ for some β we have $C_b = S_\beta$. Hence F is the set of all equivalence classes under R.

Quotient Set

The set of mutually disjoint equivalence classes in which a set S is partitioned relatively to an equivalence relation R, is called Quotient set of S for the equivalence relation R and is denoted by $\bar{S}$ or S/R

e.g the Quotient set I of all integers for the equivalence relation modulo 5 is the set $I/R = \{[0], [1], [2], [3], [4]\}$

Canonical set for an equivalence relation

A sub-set S_1 of a set S is said to be a Canonical set for an equivalence relation R in S if each member of S_1 is in the relation R to one and only one member of S. Also each member of S_1 is said to be a representative of the equivalence class to which it belongs

Thus a canonical set is a sub-set consisting of the single representatives of the equivalence classes

Illustration:- In the set of all straight lines in a plane the relation 'is parallel to' is an equivalence relation and the set consisting of lines through a pt determines a Canonical set.

Natural Mapping of S onto S/R

The mapping of S onto S/R which associates to each element a of S the equivalence class determined by a is known as the natural mapping or the canonical mapping of S onto S/R. The natural mapping is, in general, many-one in asmuch as a member of S/R is the image of all those elements of S which are in relation to 'a'.

Mapping or Function

Let X and Y be two non-empty set. Then a rule f which assigns to each element of $x \in X$, a unique element $y \in Y$ is called a mapping or a function of X into (to) Y and is denoted by

$$f : X \longrightarrow Y$$

The set X is called domain of f and the set of all the values assumed by f i.e the set $\{y \in Y / y = f(x)\}$ is called range or image set. Also Y is called the co-domain of f.

If y is image of x under f, then it is written as

$$y = f(x) \quad (f \text{ of } x)$$

f is also known as mapping or transformation or operator and x is called pre-image of y.

Function defined as sets of ordered pairs

Let X and Y be two non-empty sets. A subset f of $X \times Y$ is called a mapping or a function of X into Y if for each $x \in X$, there exists one and only one $y \in Y$ such that $(x, y) \in f$

OR

Let X & Y be two non-empty sets. A subset (Relation) f of $X \times Y$ is called function of X into Y if

(a) $\text{Dom } f = X$

(b) There is no element repeated in Dom f

Onto or Surjective mapping

If range of mapping is completely filled up, the mapping is said to be onto and if range is not completely filled up then it is into. In other words a mapping $f: X \longrightarrow Y$ is said to be onto or surjective if range of f is Y. Onto mapping is also called surjection.

one-one or Injective and Many one Mapping

Let $f: X \longrightarrow Y$ be a mapping. If two different elements of X have different images i.e f is one-one if for all $x_1, x_2 \in X$, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$

If two or more different elements of X have the same image under f, then f is said to be a many-one mapping of X into (onto) Y.

Bijective Mapping or one-to-one correspondence

A mapping which is both one-one and onto is called bijective mapping or 1-1 Correspondence or bijection.

Equal Mappings

Two mappings f, g of a set X into a set Y are are equal iff

$$f(x) = g(x) \quad \forall x \in X$$

Identity Mapping

A mapping under which every element of a set is mapped on itself is called an Identity mapping

OR

Given a non-empty set X, the identity mapping I_X on X is the mapping of X onto itself i.e $I_X : X \longrightarrow X$ and is defined as

$$I_X(x) = x \quad \forall \ x \in X$$

Inverse Mapping

Let $f: X \longrightarrow Y$ be a bijective mapping, then it is called invertible and its inverse mapping $f^{-1}: Y \longrightarrow X$ is defined as

$$\forall y \in Y,\ f^{-1}(y) = \{x : x \in X,\ f(x) = y\}$$

Inverse mapping is also bijective

Remarks

- Only bijective mapping is invertible and bijective mappings are also known as Inversible, Non-singular, Biuniform.
- Let $f: X \longrightarrow Y$. For any sub set A of X, the set $\{f(a) \mid a \in A\}$ is called image of A under f and it is denoted by $f(A)$. For any subset B of Y, the set $\{x \in X \mid f(x) \in B\}$ is subset of X, is called pre-image of B and is denoted by $f^{-1}(B)$ irrespective of whether f is or is not inversible.

  $f^{-1}(\{y\})$ denotes the set of all pre-images of $y \in Y$ of course $f^{-1}(\{y\})$ can be void in case y is not in the range of f

Theorem A function $f: X \longrightarrow Y$ is invertible if and only if $\exists$ a function $g: Y \longrightarrow X$ such that $gof = i_X$ and $fog = i_Y$, where i_X & i_Y are identity mapping on X and Y respectively

Proof Let $f: X \longrightarrow Y$ be inversible. Then by definition $\exists$ a function $g: Y \longrightarrow X$ such that $g(y) = x$ whenever $f(x) = y$, $x \in X$, $y \in Y$

For any $x \in X$, $gof(x) = g(f(x)) = g(y) = x$
$= T_x(x)$

For any $y \in Y$

$$fog(y) = f(g(y)) = f(x) = y = i_Y(y)$$

Hence $i_X = g \circ f$ and $i_Y = f \circ g$

Conversely let $g : Y \to X$ be a function such that $g \circ f = i_X$ and $f \circ g = i_Y$

Let $x_1, x_2 \in X$ and $f(x_1) = f(x_2)$

$$\Rightarrow g[f(x_1)] = g[f(x_2)]$$

$$\Rightarrow (g \circ f)(x_1) = (g \circ f)(x_2)$$

$$\Rightarrow i_X(x_1) = i_X(x_2)$$

$$\Rightarrow x_1 = x_2$$

Hence f is 1–1

Finally let $y \in Y$, then $y = i_Y(y)$

$$\Rightarrow y = (f \circ g)(y) = f(g(y))$$

as $g(y) \in X$, f is onto

Thus f is bijective and therefore inversible.

Product or Composite Mapping of two mappings

Let $f : X \to Y$ and $g : Y \to Z$ be two mappings. Then the mapping of X into Z which maps each element $x \in X$ into the g-image of the f-image of x is called Composite of f and g and is denoted by $g \circ f$

Thus $(g \circ f)(x) = g(f(x)) \quad \forall x \in X$

Associativity of Composites of Mappings

If f, g, h be mappings of S into T, T into U, U into V respectively, then $(h \circ g) \circ f = h \circ (g \circ f)$

Proof

$$[(h \circ g) \circ f](x) = (h \circ g)(f(x))$$

$$= h\{g(f(x))\}$$

$$= h\{(g \circ f)(x)\}$$

$$= \{h \circ (g \circ f)\}(x)$$

$$\Rightarrow (h \circ g) \circ f = h \circ (g \circ f)$$

Extension and Restriction of a Fun.

If $f: X \longrightarrow Y$ is a function and T is a subset of X, then function $g: T \longrightarrow Y$ is called restriction of f to T if $g(t) = f(t)$ $\forall t \in T$. We denote g by f_T. Function f is called extension of g to X.

OR

Given two functions f and g such that f contains the domain of g and $f(x) = g(x)$ $\forall x$ in the dom of g. the function f is said to be the extension of g and g is said to be the restriction of f.

Real & Complex Functions

f is said to be real or complex according as its range is real or complex.

Transformation of a set

Mapping of a set into itself is called transformation.

Permutation

A one-one mapping of a finite set onto itself is called a permutation. OR (bijective)

Given any set X, any one-to-one mapping of X onto itself is called a non-singular tranformation or permutation of X

OR

If X be a set then any one-one onto mapping $f: G \longrightarrow G$ is said to be transformation or in case G is finite, f is said to be a permutation.

Being one-one onto, a permutation is an invertible mapping

The set of all permutations of a set containing n, elements is denoted by P_n and known as the symmetric set of transformations of degree n

Number of members in the set P_n is $n!$

Cyclic Permutation

A permutation which replaces n elements cyclically is called cycle or cyclic permutation of degree n. e.g

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 2 & 3 & 4 & \cdots & n & 1 \end{pmatrix} = (123 \ldots n)$$

Transposition A cycle of length two is called a transposition.

A cycle of length one implies that the object involved is mapped on itself i.e invariant.

Denumberable set

A set X is called denumberable if it is equipotent to N, the set of natural numbers.

Countable Set

A set X is countable if either X is finite or it is equivalent to a subset of N or to the set N itself. Set X is uncountable if X is not countable Thus every denumberable set is countable but every countable set need not to be ~~countable~~ denumberable

Finite Set

A set X is said to be finite if either $X = \phi$ or X is equipotent to $\{1, 2, 3, \ldots n\}$ for some one integer n

Remark Empty set is regarded as finite set.

A set X is said to be infinite if it is equivalent to a proper subset of itself.

Illustration

The set of integers Z is infinite set as set of Even integers E is a proper subset of Z

and a function $f: Z \to E$ defined by

$f(n) = 2n \quad \forall n \in Z$ is 1-1 Correspondence

- The set Z of all integers is countable since the function defined by

$$f(n) = \begin{cases} -\frac{n-1}{2} & \text{if } n \text{ is odd} \\ \frac{n}{2} & \text{if } n \text{ is even} \end{cases}$$

is 1-1 correspondence from N to Z.

- The set of all real numbers R is uncountable and hence any interval of R is uncountable.
- The set of rational numbers is Countable
- The set of irrational numbers is uncountable.

Binary operation or Compositions

Binary operation or composition on a set X or over a set X is a mapping of $X \times X$ into X. i.e if f is a binary operation on X, then $f: X \times X \to X$.
Binary compositions are ~~usually~~ generally denoted by $\circ$ (circle) $*$, $\oplus$ or., etc.

Types of Compositions and identity

Let $*$ be a binary operation / composition on a set X. Then binary operation $*$ is

i) Commutative: if $a * b = b * a \quad \forall a, b \in X$

ii) Associative: if $a * (b * c) = (a * b) * c$

and

iii) An element e of X is said to be right identity of X w.r.t $*$ if

$$a * e = a \quad \forall a \in X$$

iv) An element e' of X is left identity of X if

$$e' * a = a \quad \forall a \in X$$

V) An element of X which is left as well as right identity is called identity of X w.r.t *

VI) If an element $\bar{a}^1$ is both left as well right inverse of a, then it is called inverse of a i.e $\bar{a}^1$ is inverse of a if

$$a * \bar{a}^1 = \bar{a}^1 * a = e$$

Algebric Structure or Algebric System

A set with one or more compositions is called algebric system or an algebric structure.

Illustrations

1: The mapping $f: Q \times Q \to Q$ defined by $f(a,b) = a+b$ is called addition composition on set Q of rational numbers

2) The mapping $f: Q \times Q \to Q$ defined by $f(a,b) = ab$ is multiplication composition.

3) Vector multiplication (Cross product) is is a composition on the set of all vectors

4) Resultant or composite of transformations is a composition on the set of all transformation.

5) Union and Intersections are two composition on power set of a set

Remark: If a set A has n members, then number of binary compositions is n^{n^2}

Proof:

Group pair $(G, \cdot)$

A system $\langle G, \cdot \rangle$ consisting of a non-empty set G and a binary composition $(\cdot)$ on G is called a group if

OR

A non-empty set G with a composition $(\cdot)$ is called group if

i) Binary operation $(\cdot)$ is associative in G i.e
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in G$$

ii) Under the binary operation $(\cdot)$ in G, there is an element e called identity in G such that
$$a \cdot e = e \cdot a = a \quad \forall a \in G$$

iii) For each $a \in G$, $\exists$ an element a' in G such that
$$a \cdot a' = a' \cdot a = e$$
i.e every element of G is inversible in G

Commutative or Abelian group

A group $(G, \cdot)$ is called commutative or Abelian gp if binary operation is commutative.

Finite & Infinite Group

A gp $(G, \cdot)$ is said to be finite if it has only a finite number of elements. Otherwise it is called infinite.

Order of a Group

The number of elements in a gp is called the order of that group. A gp is finite iff its order is finite

Order of an element

Let G be a group and $a \in G$. The least +ve integer n if it exists, such that
$$a^n = e, \text{ identity of } G$$

is called order of a. If no such integer exists, then a is said to be of infinite order. Order of identity element e in a group G is taken as 1

Periodic Group

A Group G is said to be periodic if every element of G has finite order.

Torsion Free Group

A Group G is said to be torsion free if every non-identity element of G has infinite order.

e.g Group $(Z, +)$ is torsion free
Group $(R^+, \times)$ is torsion free
Group $(Q, +)$ is torsion free.

Examples from Numbers

1. Let Z be the set of all integers, then $(Z, +)$, where $+$ is usual addition of integers is a group whereas $(Z, \cdot)$ where $\cdot$ is usual multiplication is not group because 0 has no inverse.
2) Let Q be the set of rational number, then $(Q, +)$ is a group.
If Q^* be set of all non-zero rational numbers. As the product two non zero rational numbers is rational, associative law holds, $1 \in Q^*$ and $1r = r1 = r$, $\frac{1}{r} \in Q^*$ and $r \cdot \frac{1}{r} = 1$ and $rs = sr$. Therefore Q^* is an Abelian group under multiplication.
3) Pair $(R, +)$, where R the set of real nos. is a group.
But R is not group with multiplication.
4) $(C, +)$ is a group but C is not gp under multiplication.
5) The set of +ve rational real no (real or complex) form gp under multiplication

6: The set of n-nth roots of unity with multiplication composition is a finite abelian gp

Here By cde. Moivre's theorem $1/n$

$$(1)^{1/n} = (\cos 2\pi k + i \sin 2\pi k)$$
$$= \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}$$

where $k = 0, 1, 2, \ldots n-1$

So n, nth roots of unity are

$$G = \{1, \cos \tfrac{2\pi}{n} + i \sin \tfrac{2\pi}{n}, \cos \tfrac{2\cdot 2\pi}{n} + i \sin \tfrac{2\cdot 2\pi}{n} \ldots$$
$$, \cos \tfrac{(n-1)}{n} 2\pi + i \sin \tfrac{(n-1)}{n} 2\pi \}$$

$$= i.e \{1, e^{\frac{2\pi i}{n}}, e^{\frac{2\cdot 2\pi i}{n}}, e^{\frac{3\cdot 2\pi i}{n}}, \ldots e^{(n-1)\frac{2\pi i}{n}} \}$$

(i) Set $a = e^{p\cdot\frac{2\pi i}{n}}$, $b = e^{q\cdot\frac{2\pi i}{n}} \in G$

where $0 \le p \le n-1$, $0 \le q \le n-1$

Then

$a.b = e^{(p+q)\frac{2\pi}{n} i}$ will be in G

if $p+q \le n-1$.

Suppose on contrary $p+q > n-1$ so that $p+q = n+m$ where $m \le n-2$ since the max value of $p+q$ can be $2(n-1)$ i.e $2n-2$

$$\therefore a.b = e^{(m+n)\frac{2\pi i}{n}} = e^{2\pi i} \cdot e^{2\pi i \, m/n} = e^{\frac{m}{n} 2\pi i}$$

$\because e^{2\pi i} = \cos 2\pi + i \sin 2\pi = 1$

which follows that $a.b \in G$ since $m \le n-2$

ii) Associative law holds since multiplication of Complex numbers is associative.

iii) 1 is identity and the inverse of $e^{\frac{2\pi k i}{n}}$ is the number $e^{\frac{2\pi i(n-k)}{n}}$ since

$$e^{\frac{2\pi i k}{n}} \cdot e^{2\pi i(n-k)/n} = e^{\frac{2\pi i n}{n}} = e^{2\pi i} = e = 1$$

7: The set $C_4 = \{\pm 1, \pm i\}$ under complex multiplication is a gp.

8: $(Q', \cdot)$, $(R', \cdot)$ and $(C', \cdot)$ where Q', R', C' are non zero real, complex and rational numbers are group.

9: **Additive gp of Integers modulo m I_m**

The set $I_m = \{0, 1, 2, \ldots m-1\}$ with binary composition defined by

$a + b = r$ where r is least +ve integer obtained when $a+b$ is divided by m, is gp.

(i) This composition is associative because $a+(b+c)$ & $(a+b)+c$ both denote the remainder obtained on dividing the ordinary sum of a, b, c by m

ii) 0 is identity because for and $a \in I_m$, $0 \leq a < m$ and $a + a = a + 0 = 0m + a$ gives that a is least +ve integer obtained by dividing a by m

iii) Inverse: For any $a \in I_m$ if $a = 0$, then $0 + 0 = 0$

If $a \neq 0$ then as $0 < m - a < m$, $m - a \in I_m$.

Further $(m-a) + a = a + (m-a) = m + 0 = 0$

So that $m - a$ is inverse of a.

Thus in particular $I_3 = \{0, 1, 2\}$ $I_4 = \{0, 1, 2, 3\}$ etc are group

Multiplicative gp of integers modulo a prime p

Consider a set

$Z'_p = \{0, 1, 2, \ldots p-1\}$, where p is prime.

Define multiplication in Z'_p as

For $a, b \in Z'_p$

$a \cdot b = r$ where r is remainder obtained by dividing $a \cdot b$ by p

i) Associative law: The composition is associative as $(ab)c$ as well as $a(bc)$ denote the least +ve integer remainder obtained on dividing the ordinary product of a, b, c by p

ii) 1 is identity element

iii) Let $a \in Z_p$. Consider the products

$1a, 2a, 3a \ldots\ldots, (p-1)a$

No two of these can be equal so that one of these must equal 1. Thus if $aa' = 1$, Then a' is inverse of a.

Thus the set is gp (Abelian) of order $p-1$

10 Let $S = \{x \in Z \mid 1 \leq x \leq n, \text{and}(x, n) = 1\}$

Define multiplication of $a, b \in S$ as $ab = r$, where is remainder when ab is divided by n. Then S is gp under multiplication.

(i) Closure law:

Let $a, b \in S$ and $ab = c$. Then c can not be zero otherwise n/ab which is absurd as $(a, n) = 1$ $(b, n) = 1$, so $1 \leq c < n$.

Further if $(c, n) \neq 1$, then $\exists$ a prime p such that p/c & $p/n \Rightarrow p/ab \Rightarrow ab = kp + c$

$\therefore p$ is prime, p/a or p/b. Thus either p divides HCF of a, n or HCF of b, n which is impossible as $(a, n) = 1 = (b, n)$. Thus $(c, n) = 1$. Hence $c \in S$ and Composition is closed in S

ii) Associative law:- The composition is associative because $(ab)c$ & $a(bc)$ are both least +ve integers obtained by dividing $(ab)c$ & $a(bc)$ by n

OR Let $ab = r_1$ and $(ab)c = r_1c = r_2$

$\Rightarrow r_1c = r_2 + k_2 n$ for some integer k_2

Now $ab = r_1 \Rightarrow ab = r_1 + k_1 n$ for some integer k_1

So $r_1c = r_2 + k_2 n$.

$\Rightarrow (ab - k_1 n)c = r_2 + k_2 n$.

$(ab)c = r_2 + (k_2 + k_1 c) n$.

$\Rightarrow r_2$ is the least +ve remainder got on dividing $(ab)c$ by n. Similarly if $a(bc) = r_3$, then r_3 is the least +ve integer obtained as remainder when $a(bc)$ is divided by n.

iii) Identity:- Let $a \in S$ then $1a = a1 = a$

so 1 is identity of S

iv) Inverse:- Let $a \in S \Rightarrow (a, n) = 1$

So there exist integers x and y such that

$ax + by = 1$ if $1 \leq x < n$ and $(x, n) = 1$, $x \in S$

If not, then by division algorithm there exists integers q & r such that

$x = qn + r$, $0 \leq r < n$

Now $ax + ny = 1$

$\Rightarrow aqn + ar + ny = 1$

$\Rightarrow ar = 1 + (-aq - y)n$

$\Rightarrow ar = 1 \pmod n$

Similarly $ra = 1 \pmod n$

Now if $(r, n) \neq 1$, let p be a prime no dividing r and n. Then p will divide x so $p \| 1$ as $ax + ny = 1$, which is absurd. Therefore $(r, n) = 1$, hence $r \in S$

Thus S is group under multiplication mod m

$Z_p = \{1, 2, 3, \ldots p-1\}$ is gp under multiplication

$4 \{2, 4, 6, \ldots 2(p-1)\}$ where p's

$p = p > 2$ is gp $\times_{2p}$

Group of Vectors

i) The set of all vectors with vector addition as the composition is an infinite abelian gp.

ii) The set of all coplanar vectors is an infinite abelian gp under addition.

Group of Matrices

i) The set of all $m \times n$ matrices having their elements as integers (rational, real or complex) is an infinite abelian gp with matrix addition as composition. $M_{m\times n}(\mathbb{R})$

ii:- The set of all $n \times n$ non-singular matrices having their elements as rational (real or complex) is an infinite non-abelian gp with matrix multiplication as composition $GL(n,\mathbb{R})$ degree $SL(2,\mathbb{R})$

Note The set of $n \times n$ non-singular matrices having elements as ~~rational~~ integers is not a gp for matrix multiplication for, not all such matrices are inversible e.g matrix

$$\begin{bmatrix} 1 & 2 \\ 3 & 2 \end{bmatrix}$$ whose det is -4 is non-singular but non-invertible in integers because its inverse is

$$\begin{bmatrix} -1/2 & 1/2 \\ 3/4 & -1/4 \end{bmatrix}$$

If $A_2 \begin{bmatrix} a & b \\ c & d \end{bmatrix}$

Adj $A_2 \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

Group of Transformations

b) Alternating gp (a) Symmetric gp

(a) :- The set P of all permutations of degree n is a finite non-abelian gp of order $n!$

(b) :- Alternating group A_n of degree n

The set A_n of all even permutations of degree n is a finite non-abelian gp. known

as the alternating group of order $\frac{1}{2}n!$

Consider the set
$\{f_1, \ldots\ldots, f_k\}$ of members of A_n. $\rightarrow$①
Let
$f = (ab)$ be any transposition
Then each of the members of the set
$\{f_1 \circ f, \ldots\ldots f_k \circ f\}$ is an odd $\rightarrow$②
permutation. In fact
$f_i \circ f = f_j \circ f \Rightarrow (f_i \circ f) \circ f = (f_j \circ f) \circ f$
$\Rightarrow f_i \circ (f \circ f) = f_j \circ (f \circ f)$
$\Rightarrow f_i = f_j$

Also any odd permutation, g, can be written as the product of an even permutation with f
in fact
$g = g \circ (f \circ f) = (g \circ f) \circ f$

Thus the two sets ① & ② exhaust all the permutations of P_n and accordingly
$k = \frac{1}{2}n!$ $\quad 2k = n!$, $k = \frac{1}{2}n!$

(c) The set of all bilinear transformation of infinite complex plane is an infinite non-abelian group. Let z denote any complex number. Then bilinear transformation is given by

$f: C \rightarrow C : f(z) = \frac{az+b}{cz+d}$, $ad - bc \neq 0$, $a, b, c, d \in C$

It may be shown that this is a one-one mapping of the infinite complex plane onto itself
Let f & g be two bilinear transformations defined by

$f: C \rightarrow C : f(z) = \frac{az+b}{cz+d}$ $\quad ad - bc \neq 0$

$g : C \to C : g(z) = \frac{\alpha z + \beta}{\gamma z + \delta}$, $\alpha\delta - \beta\gamma \neq 0$

we have

$(g \circ f)(z) = g[f(z)] = g\left(\frac{az+b}{cz+d}\right)$

$$= \frac{\alpha[(az+b)/(bz+c)] + \beta}{\gamma[(az+b)/(bz+c)] + \delta}$$

$$= \frac{(a\alpha + c\beta)z + (b\alpha + d\beta)}{(a\gamma + c\delta)z + (b\gamma + d\delta)}$$

Here

$$(a\alpha + c\beta)(b\gamma + d\delta) - (b\alpha + d\beta)(a\gamma + c\delta)$$
$$= (ad - bc)(\alpha\delta - \beta\gamma) \neq 0$$

Thus $(g \circ f)$ is a bilinear transformation.

Also the transformation given by

$e : C \to C : e(z) = \frac{1z+0}{0z+1}$

which is bilinear is the identity transformation.

Finally, the transformation h given by

$h : C \to C : h(z) = \frac{b - dz}{cz - a}$.

is inverse of f

$(h \circ f)z = h(f(z)) \to h\left(\frac{az+b}{cz+d}\right)$

$$= \frac{b - d[(az+b)/(cz+d)]}{c[(az+b)/(cz+d)] - a} = z$$
$$= e(z)$$

So $h \circ f = e$

Similarly $f \circ h = e$

(d) The set of six special bilinear mappings $f_1, f_2, f_3, f_4, f_5, f_6$ defined by

$f_1(z) = z$, $f_2(z) = \frac{1}{z}$, $f_3(z) = 1 - z$

$f_4(z) = \frac{z}{z-1}$; $f_5(z) = \frac{1}{1-z}$, $f_6(z) = \frac{z-1}{z}$

is a finite non-abelian gp of order 6

Group of Quaternians

The quaternions $\pm I, \pm i, \pm j, \pm k$ satisfying the equations $i^2 = j^2 = k^2 = -I$, $ij = k, jk = i, ki = j$ $ji = -k$ $kj = -i$, $ik = -j$ form a gp Q called the group of quaternions. This is non-abelian gp of order 8.

Elementary Properties of a Group

Theorem:- Let G be a gp. Then.

(i) :- Identity element of G is unique

(ii) :- Every $a \in G$ has unique inverse in G

(iii) :- For all $a, b, c \in G$ $\quad ab = ac \Rightarrow b = c$ & $ba = ca \Rightarrow b = c$

(iv) :- If $a, b \in G$, then the equation $ax = b$, $ya = b$ have unique sols. i.e for any pair of elements a, b in G, $\exists$ unique elements x, y of G such that $ax = b$, $ya = b$

(v) :- For every $a \in G$, $(a^{-1})^{-1} = a$

(vi) : For all $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$

Proof:-

(i) Uniqueness of identity

Let e & e' be two identity elements of G, then

$$ea = ae = a \quad \forall a \in G \longrightarrow (1)$$

and $$e'a = ae' = a \quad \forall a \in G \longrightarrow (2)$$

$$\Rightarrow ea = e'a \Rightarrow e = e'$$

Also $$\Rightarrow ae = ae' \Rightarrow e = e'$$

OR

$$ee' = e'e = e' \quad \because e \text{ is identity}$$

and $$e'e = ee' = e \quad \because e' \text{ is " "}$$

$$\Rightarrow e = e'$$

Hence identity element of gp G is unique.

(ii) : Uniqueness of Inverse :-

Let an element $a \in G$ has two inverses x & y in G. Then

$$xa = ax = e \longrightarrow ①$$
$$ya = ay = e \longrightarrow ②$$

$$\Rightarrow x = xe = x(ay) = (xa)y = ey = y$$

Hence the inverse of a is unique.

Aliter

$$xa = ax = e \longrightarrow ①$$
$$ya = ay = e \longrightarrow ②$$

pos-multiplying ① by y

$$(xa)y = (ax)y = y \longrightarrow ③$$

Pre-multiplying ② by x

$$x(ya) = x(ay) = x \longrightarrow ④$$

But $(xa)y = x(ay)$ (Associative law)

$$y = x$$

Hence uniqueness

(iii) Cancellation Laws :-

(a) we have $ab = ac$

Let $\bar{a}^1$ be inverse of a in G, then

$$\bar{a}^1(ab) = \bar{a}^1(ac)$$
$$\Rightarrow (\bar{a}^1 a)b = (\bar{a}^1 a)c \quad \text{(Associative law)}$$
$$\Rightarrow eb = ec$$
$$\Rightarrow b = c$$

(b) Given $ba = ca$

$$\Rightarrow (ba)\bar{a}^1 = (ca)\bar{a}^1$$
$$\Rightarrow b(a\bar{a}^1) = c(a\bar{a}^1)$$
$$\Rightarrow be = ce$$
$$\Rightarrow b = c$$

Remark In a semi-group cancellation law may not hold.

(IV) Uniqueness of Solutions

$ax = b \rightarrow (a)$ $\quad ya = b \rightarrow (b)$

If $\bar{a}^1$ be the inverse of in G, then $a\bar{a}^1 = e$.

Now $\bar{a}^1 \in G$ and $b \in G \Rightarrow \bar{a}^1 b \in G$

putting $\bar{a}^1 b$ in equation $ax = b$ we get

$$ax = a(\bar{a}^1 b) = (a\bar{a}^1)b = b = R.H.S$$

$\Rightarrow x = \bar{a}^1 b$ is a sol of $ax = b$

To show that sol is unique. Let x' is another sol in G, then

$$ax' = b = eb = (a\bar{a}^1)b = a(\bar{a}^1 b)$$

$\Rightarrow ax' = a(\bar{a}^1 b)$

$\Rightarrow x' = \bar{a}^1 b$ (left cancellation Law)

$\Rightarrow x' = \bar{a}^1 b = x$

i.e solution is unique.

Again $b \in G$ and $\bar{a}^1 \in G \Rightarrow b\bar{a}^1 \in G$

putting $y = b\bar{a}^1$ in $ya = b$ we get

$$(b\bar{a}^1)a = b(\bar{a}^1 a) = b = R.H.S$$

$\Rightarrow y = b\bar{a}^1$ is a sol of $ya = b$

To show that this sol is unique let z be different sol in G, then

$$za = b = be = b(\bar{a}^1 a) = (b\bar{a}^1)a$$

$\Rightarrow z = b\bar{a}^1$ (Right cancellation Law)

$\Rightarrow z = y$ and hence the sol is unique.

(V) Inverse of the inverse itself

Since for any $a \in G$, $a\bar{a}^1 = \bar{a}^1 a = e$.

$$\Rightarrow (\bar{a}^1)^{-1} = a$$

OR

Inverse Law gives

$$(\bar{a}^1)^{-1}\bar{a}^1 = e$$

$$[(\bar{a}^1)^{-1}\bar{a}^1]a = ea$$

$$(\bar{a}^1)^{-1}(\bar{a}^1 a) = a$$

$$(\bar{a}^1)^{-1}(e) = a$$

$$(\bar{a}^1)^{-1} = a$$

vi. Reversal Law

$$(ab)(b^{-1}a^{-1}) = [a(bb^{-1})]a^{-1}$$
$$= (ae)a^{-1}$$
$$= aa^{-1} = e$$

Also $(b^{-1}a^{-1})(ab) = b^{-1}[(a^{-1}a)b]$
$$= b^{-1}b = e.$$

Hence
$$(ab)^{-1} = b^{-1}a^{-1}$$

Note This result may be generalized for any number of elements $a_1, a_2, \ldots a_n \in G$, as
$$(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}$$

This means that the inverse of the product of any number of elements is equal to the product of their inverses taken in the reverse order

Problems Concerning Group

Problem 1 Show that the three cube roots of unity form a abelian finite group under multiplication

Solution We have $G = \{1, \omega, \omega^2\}$, where $\omega^3 = 1$

(i) Since all the elements in composition table belong to G, closur law holds in G.

(ii) Since multiplication of complex is associative, associative law holds

(iii) 1 is identity of G

(iv) Inverse of $1, \omega, \omega^2$ are $1, \omega^2, \omega \in G$

(v) Commutative property is satisfied as

·	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	$\omega^3 = 1$
ω^2	ω^2	1	$\omega^4 = \omega$

$\omega^4 = \omega^3\omega = 1 \cdot \omega = \omega$

$1 \cdot \omega = \omega \cdot 1 = \omega \in G$

$1 \cdot \omega^2 = \omega^2 \cdot 1 = \omega^2 \in G$

$\omega \cdot \omega^2 = \omega^2 \cdot \omega = \omega^3 = 1 \in G$

Problem 2: Show that the set of matrices

$$A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$$, where α is real

form a gp under multiplication

Solution:

Let G_1 be the set of all matrices and $A_\alpha, A_\beta, A_\gamma \in G_1$, then

(i) $$A_\alpha \cdot A_\beta = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix}$$

$$= \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix} = A_{\alpha+\beta},\ \alpha+\beta \text{ is real}$$

$\Rightarrow A_{\alpha+\beta} \in G_1$

(ii) $A_\alpha \cdot (A_\beta \cdot A_\gamma) = A_\alpha \cdot A_{\beta+\gamma} = A_{\alpha+\beta+\gamma} = A_{\alpha+\beta} \cdot A_\gamma$

(iii) $A_{-\alpha}$ is inverse of $\forall A_\alpha \in G_1$ because

$A_{-\alpha} \cdot A_\alpha = A_{-\alpha+\alpha} = A_0 =$ Indentity matrix

(iv) $A_\alpha \cdot A_\beta = A_{\alpha+\beta} = A_{\beta+\alpha} = A_\beta \cdot A_\alpha$

Hence given set of matrices forms an Abelian gp

Problem 3: If OX, OY be the two rectangular axes in the cartesian plane and T_α denotes the the rotation of the axes through an angle α s.t that

$T_\alpha : (x, y) \longrightarrow (x\cos\alpha + y\sin\alpha, -x\sin\alpha + y\cos\alpha)$

then show that the set of these rotations w.r.t operation $\circ$, s.t that $T_\beta \circ T_\alpha$ is the resultant of two such operations, forms a gp.

Solution:-

Let $G_1 = \{ T_\alpha : (x, y) \longrightarrow (x\cos\alpha + y\sin\alpha, -x\sin\alpha + y\cos\alpha) \}$

(i) Let $T_\beta, T_\alpha \in G_1$

$T_\beta \circ T_\alpha (x, y) = T_\beta [T_\alpha (x, y)]$

$= T_\beta [x\cos\alpha + y\sin\alpha, -x\sin\alpha + y\cos\alpha]$

$= ((x\cos\alpha + y\sin\alpha)\cos\beta + (-x\sin\alpha + y\cos\alpha)\sin\beta, -(x\cos\alpha + y\sin\alpha)\sin\beta + (-x\sin\alpha + y\cos\alpha)\cos\beta)$

$= (x\cos(\alpha+\beta) + y\sin(\alpha+\beta), -x\sin(\alpha+\beta) + y\cos(\alpha+\beta))$

$= T_\alpha \circ T_\beta (x, y)$ for any (x, y) in the plane

(iii) Set $T_\alpha, T_\beta, T_\gamma \in G_7$ then

$T_\gamma \circ (T_\beta \circ T_\alpha) = T_\gamma [x\cos(\alpha+\beta) + y\sin(\alpha+\beta), -x\sin(\alpha+\beta) + y\cos(\alpha+\beta)]$

$= T_{\alpha+\beta+\gamma}$

$= [x\cos(\alpha+\beta+\gamma) + y\sin(\alpha+\beta+\gamma), -x\sin(\alpha+\beta+\gamma) + y\cos(\alpha+\beta+\gamma)]$

$= (T_\alpha \circ T_\beta) \circ T_\gamma$

(iv) T_0 is identity of G_7.

(v) $T_{-\alpha} \in G_7$ and $T_{-\alpha} \circ T_\alpha = T_0 \quad \forall\ T_\alpha \in G_7$

(vi) Commutative law also holds.

Hence G_7 an abelian gp

Problem: 4 Prove that the residue classes modulo m form a gp w.r.t addition of residue classes

Solution

Set G_7 be the set of residue classes modulo m

$G_7 = \{[0], [1], [2], \ldots\ldots [m-1]\}$

(i) Set $[r_1], [r_2] \in G_7$, then

$[r_1] + [r_2] = [r_1 + r_2] = [r] \in G_7 \quad 0 \le r < m$ and $r_2 + r_3 = mk + r$

(iii) If $[r_1] [r_2] [r_3] \in G_7$

so that

$r_1 + r_2 + r_3 = r_1 + mk + r$

$= mk + r_1 + r = mk + r'$

where r' is least one integer remainder when $r_1 + r_2 + r_3$ is divided by m

Then

$$[r_1] + ([r_2] + [r_3]) = [r_1] + [r_2 + r_3]$$
$$= [r_1] + [r_2 + r_3]$$
$$= [r_1] + [r]$$
$$= [r_1 + r] = r'$$
$$= [r_1 + r_2 + r_3]$$
$$= [r_1 + r_2] + [r_3]$$
$$= ([r_1] + [r_2]) + [r_3]$$

$\Rightarrow$ Addition of residue classes is associative

(iv) $[0] \in G_1$ is additive identity because
$[0] + [r] = [r] \quad \forall [r] \in S$

(v) $\forall [r] \in G_1 \; \exists$ inverse $[m-r]$ such that
$[r] + [m-r] = [m] = [0] \quad \forall [r] \in G_1$

Hence the set of residue classes is gp under addition.

Problem 5:- Prove that the non-zero residue classes modulo m (a prime integer) w.r.t multiplication form a group

Solution:- Let G_1 be the set of non-zero residue classes modulo m, then we have
$G_1 = \{[1], [2], \ldots [r] \ldots [m-1]\} \quad 0 < r \leq m-1$

(i) Since multiplication of $[r_1], [r_2], [r_3] \in G_1$ is defined by
$[r_1][r_2] = [r_3]$, where $0 < r_1, r_2, r_3 \leq m-1$
and r_1, r_2 are prime to m so division of $r_1 r_2$ by m renders a non-zero remainder and so if $[r_1], [r_2] \in G_1$, then
$[r_1][r_2]$ i.e $[r_3] \in G_1$

(II) Set $[r_1], [r_2], [r_3] \in G_r$ and $r_1 r_2 = mk + r$ Then

$(r_1 r_2) r_3 = (mk + r) r_3 = mk r_3 + r r_3 = p + r'$

so that

$([r_1] \cdot [r_2]) \cdot [r_3] = [r_1 r_2][r_3] = [r][r_3]$ $\because r_1 r_2 \equiv r \pmod m$

$= [r r_3] = [r']$ $r r_3 \equiv r' \pmod m$

But $r_1 r_2 r_3 \equiv r' \pmod m$

$\therefore [r'] = [r_1 r_2 r_3] = [r_1][r_2 r_3] = [r_1] \cdot ([r_2] \cdot [r_3])$

i.e. $([r_1] \cdot [r_2]) \cdot [r_3] = [r_1]([r_2][r_3])$

$\Rightarrow$ associative law holds

(III) $[1] \in G_r$ is identity because

$[1][r] = [r] \quad \forall r \in S$

(IV) Inverse:-

Multiplying each element of G_r by an element $[r]$, we have.

$[1][r], [2][r], \dots, [m-1][r]$ ⟶ ①

By closure law all these elements must belong to G_r. Also all of them must be distinct otherwise if

$[r_1][r] = [r_2][r]$

Then $[r_1] = [r_2]$ which contradicts the hypothesis that $[r_1], [r_2]$ are distinct. Hence all $(m-1)$ elements must be distinct and they must also be the same elements of G_r as already defined except that their order may be different. Conclusively in ① there is one elemet which is identity $[1]$. Suppose this identity element is $[r_1][r]$ i.e

$[r_1][r] = 1$

$\Rightarrow [r_1]$ is inverse of $[r]$. But r being arbitrary, the inverse of each element exists. Hence the non-zero residue classes modulo

m w.r.t multiplication form a group.

• **Problem: 6:-** If G be a gp and $\bar{a}^1 = a \ \forall a \in G$, then G is ablian. OR If every element of gp G is its own inverse, then show that G is abelian.

Solution:- Given that G is a gp.

Let $a, b \in G$

$\Rightarrow \bar{a}^1, b^{-1} \in G$ and $\bar{a}^1 = a$, $b^{-1} = b$

$(ab)^{-1} = b^{-1}\bar{a}^1 = ba$

But $(ab)^{-1} = ab$

$\Rightarrow ab = ba$

$\Rightarrow G$ is abelian gp.

Problem: 7:- If G be a gp and $a^2 = e \ \forall a \in G$, then show that the gp must be commutative

Solution: Given that G is a gp

and $a^2 = e$

$a.a = e \Rightarrow a = \bar{a}^1$

Let $a, b \in G \Rightarrow a = \bar{a}^1$ & $b = b^{-1}$

$(ab)^{-1} = b^{-1}\bar{a}^1 = ba$

$ab = ba$

Problem: 8:- Show that if a gp has 3, 4, or 5 elements, then it is abelian

Solution We prove for 4 elements, similar procedure can be adopted for the other two

Suppose that $G = \{e, a, b, c\}$ is set forming gp G, where e is the identity element.

Case I In case every element of G is its own inverse, then G is abelian

Case II If every element of G is not its own inverse.

Let $\bar{a}^1 = b$, then the only alternative is that $\bar{c}^1 = c$ so that

$ab = ba = e$ & $\bar{c}^1 = c \Rightarrow cc = e$

Now

$ac \neq e$ as $c^{-1} \neq a$

$ac \neq a$ as $c \neq e$

$ac \neq c$ as $a \neq e$

So the only alternative is $ac = b$

Similar argument will give that

$ca = b$

$\therefore ac = ca$

:	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

Also

$bc \neq e$ as $b^{-1} \neq c$

$bc \neq b$ as $c \neq e$

$bc \neq c$ as $b \neq e$

$\Rightarrow bc = a$ and similarly $cb = a$

$\Rightarrow bc = cb$

Hence G is abelian gp

Problem: 9: Show that any non-commutative gp has at least six elements.

Solution:-

Let G be non-commutative gp. It will be so if it has at least one pair of non-commuting elements a & b (say).

We shall first show that a set $\{e, a, b, ab, ba\}$ having a, b non-commuting elements i.e $ab \neq ba$ consists of distinct elements

Taking two at a time, there are ten possibilities leading to a contradiction of $ab \neq ba$

(i) $e = a \Rightarrow ab = eb = b = be = ba$

$\Rightarrow ab = ba$ (Contradiction to $ab \neq ba$)

(ii) $e = b \Rightarrow ab = ae = ea = ba$.

(iii) $e = ab \Rightarrow ae = ea = (ab)a = a(ba)$

$\Rightarrow e = ba$ or $ab = ba$

(iv) $e = ba \Rightarrow ea = ae = a(ba) = (ab)a$ i.e

$e = ab$ or $ba = ab$

(v) $a = b \Rightarrow ab = aa = ba$

(vi) $a = ab \Rightarrow e = b$ (thereby reducing to ii)

(vii) $b = ab \Rightarrow e = b$ (reducing to ii)

(viii) $b = ab \Rightarrow e = a$ (" " to i)

(ix) $b = ba \Rightarrow e = a$ (" " to i)

(x) $\therefore ab = ba$

Hence elements of set $\{e, a, b, ab, ba\}$ are distinct

We shall now show that at least one the gp elements aa or aba is distinct from these five namely e, a, b, ab, ba

To show that aa is different from each element a, b, ab, ba we see that

(xi) $aa = a \Rightarrow a = e$ (redees to i)

(xii) $aa = b \Rightarrow ab = a(aa) = (aa)a = ba$

(xiii) $aa = ab \Rightarrow a = b$ reducing to v

(xiv) $aa = ba \Rightarrow a = b$ " " "

$\Rightarrow$ Either $aa \neq e$ in which case aa is sixth element of G_1 or else $aa = e$.

Again we shall show that ~~$a(ba)$~~ aba is different from e, a, b, ab, ba and so it will be the sixth element of G_1

Now consider the case

(xv) $aba = e \Rightarrow ba = a(aba) = ae = a$

$\Rightarrow ba = a \Rightarrow b = e$ (reducing to viii)

(xvi) $aba = a \Rightarrow ab = e$ (reducing to iii)

(xvii) $aba = b \Rightarrow ab = a(aba) = ba$ when $aa = e$

(xviii) $aba = ab \Rightarrow a = e$ reducing to (i)

(xix) $aba = ba \Rightarrow a = e$ " " "

Conclusively a gp upto 5 elements is essentially abelian but for it to be non-abelian there should be at least six elements.

Problem :10:- If in a gp G, $xy^2 = y^3x$ and $yx^2 = x^3y$, then show that $x = y = e$, where e is identity of G.

Solution :- $xy^2 = y^3x$

$\Rightarrow x = y^3xy^{-2}$

$x^2 = x \cdot x = xy^3xy^{-2} = xy^2yxy^{-2} = xy^2yxy^{-2}$

$= y^3xyxy^{-2}$

$\Rightarrow x^2y = y^3xyx^{-1}$ ——— ①

Now $yx^2 = x^3y \Rightarrow yx^2x = xy^3xyx^{-1}$

$\Rightarrow x^2 = y^{-1}xy^3xyxy^{-1}$

$x^2y = y^{-1}xy^3xyx$ ——— ②

By ① & ②

$y^3xyxy^{-1} = y^{-1}xy^3xyx$

$\Rightarrow y^4xyx = xy^3xyxy$

$\Rightarrow y^4xyx = xy^2yxyxy = y^3xyxyxy$

$\Rightarrow (yx)^2 = (xy)^3$ ——— ③.

Interchanging x & y in ③

$(xy)^2 = (yx)^3$ ——— ④

③ & ④ $\Rightarrow$

$(xy)^2 = (yx)^3 = (yx)^2(yx) = (xy)^3(yx)$

$\Rightarrow e = xy^2x \Rightarrow x^{-2} = y^2$

Further $xy^2 = y^3x \Rightarrow xx^{-2} = yy^{-2}x$

$\Rightarrow x^{-1} = yx^{-1} \Rightarrow y = e$

Lastly $yx^2 = x^3y \Rightarrow ex^2 = x^3e \Rightarrow x = e$

Hence $x = y = e$.

Problem :11:- (Is bell) G is a gp and there exist two relatively prime positive integers m and n such that $a^mb^m = b^ma^m$ and $a^nb^n = b^na^n$ $\forall a, b \in G$. Prove that G is Abelian.

Solution: Since $(m, n) = 1$

$\Rightarrow mx + ny = 1$ for some $x, y \in \mathbb{Z}$

Now $(a^m b^n)^{mx} = a^m (b^n a^m)^{mx-1} b^n$

$= a^m (b^n a^m)^{mx} (b^n a^m)^{-1} b^n$

$= (b^n a^m)^{mx} a^m a^{-m} b^{-n} b^n$

$= (b^n a^m)^{mx}$ ⟶ ①

Similarly it can be proved that

$(a^m b^n)^{ny} = (b^n a^m)^{ny}$ ⟶ ②

from ① & ② we get

$a^m b^n = (a^m b^n)^{mx+ny}$

$= (b^n a^m)^{mx+ny} = b^n a^m$ ⟶ ③

$ab = a^{mx+ny} b^{mx+ny}$

$= a^{mx} (a^{ny} b^{mx}) b^{ny}$

$= a^{mx} (b^{mx} a^{ny}) b^{ny}$

$= a^{mx} b^{mx} a^{ny} b^{ny}$

$= b^{mx} \cdot a^{mx} \cdot b^{ny} \cdot a^{ny}$

$= b^{mx+ny} a^{mx+ny}$

$= ba$

Hence G is Abelian.

Problem : 12 If G is a gp in which $(ab)^i = a^i b^i$ for three consecutive integers i and for all $a, b \in G$ Show that G is Abelian. Given an example to show that this result doesn't hold for semi-group.

Solution :-

Problem: 13 Show that the equation $x^2ax = \bar{a}^1$ is solvable in G, for x iff a, is cube of some element in G.

Solution: Let $x^2ax = \bar{a}^1$ is solvable in G, there exists $c \in G$ such that $c^2ac = \bar{a}^1$

$\Rightarrow$ $cacac = \bar{c}^1$

$\Rightarrow$ $cacac = e$

$\Rightarrow$ $cacacca = ea = a$

$\Rightarrow$ $(ca)^3 = a$

Conversely let $a = b^3$ for some $b \in G$. Then $x = b^{-2}$ is a solution of $x^2ax = \bar{a}^1$, since

$x^2ax = b^{-4}b^3b^{-2} = b^{-3}$ while $\bar{a}^{-1} = b^{-3}$

Theorem:- Let G be a gp and $a \in G$. If order of a is n i.e $a^n = e$, then $a^k = e$ iff k is divisible by n i.e $k = qn$ or n/k.

Proof:-

Let $a^k = e$

and $k = nq + r \quad 0 \leq r < n$

$$e = a^k = a^{nq+r}$$
$$= (a^n)^q \cdot a^r$$
$$= e \cdot a^r = a^r$$

But since $o(a) = n$ and $r < n$

$\therefore r = 0$ because otherwise a will have order a number smaller than n.

Hence $k = nq$

$\Rightarrow n/k$

Conversely let $k = nq$ i.e n/k we prove that $a^k = e$

$$a^k = a^{nq} = (a^n)^q = e^q = e$$

Remark If $o(a) = n$, then the elements $a^0, a, a^2, \ldots a^{n-1}$ are distinct.

Theorem:- The order of every element of a finite group is finite.

Proof:- Let a be an element of a gp G of finite order, then the +ve integral powers viz $a, a^2, a^3, a^4 \ldots$ will all be the members of G.

$\because$ order of G is finite

$\therefore$ All these elements can not be different

Suppose that

$$a^r = a^s \quad r > s$$
$$a^{r-s} = a^r a^{-s} = a^s \cdot a^{-s} = a^0 = e$$

$\Rightarrow$, e being the identity of G.

If $r-s=m$, then $a^{r-s} = e \Rightarrow a^m = e$, m being +ve integer as $r > s$

Thus follows that $\exists$ a +ve integer m s.t $a^m = e$

As every set of +ve integers essentially have a least member so the set of all those +ve integers m s.t $a^m = e$ has a least member known as the order of a. But a is arbitrary and hence the order of every element of G is finite.

Theorem: Show that the order of any power of any element (a) of a group is atmost equal to the order of the element.

Proof:-

Let $o(a) = m$ & $o(a^p) = n$, $p \in I$

$\Rightarrow a^m = e$

$\Rightarrow (a^m)^p = e^p = e$.

$\Rightarrow (a^p)^m = e$.

$\Rightarrow$ order of $(a^p) \leq m$.

Hence proved.

Theorem: In a group G, following hold

(i) For any two elements $a, x \in G$, $o(a) = o(x^{-1}ax)$

(ii) For any $a \in G$ $o(a) = o(a^{-1})$

(iii) For any two elements $a, b \in G$ $o(ab) = o(ba)$

(iv) If for any $a \in G$, $o(a)$ is finite, then for any integer m, $a^m = e \Rightarrow o(a) / m$

(v) If $o(a) = n$ and a +ve integer k/n, then $o(a^k) = n/k$

Proof:- (i) Let n be any +ve integer such that

$a^n = e$

$\Leftrightarrow x^{-1}a^n x = x^{-1}ex = e$

$\Leftrightarrow (x^{-1}ax)^n = e^n = e$

$\Rightarrow (x^{-1}ax)^n = x^{-1}a^n x$

Consequently $o(x^{-1}ax) = o(a)$

(iii) Since $ab = b^{-1}b\,ab = b^{-1}(ba)\,b$ ——

$\Rightarrow \quad o(ab) = o(ba)$

(ii)

Let $o(a) = m$ $\quad o(\bar{a}^1) = n$

$\Rightarrow a^m = e$ $\quad (\bar{a}^1)^n = e.$

Now $\bar{a}^1$ being an exponent power of a. Since order of any power of any element of gp is atmost equal to order of the element.

$\therefore \quad o(\bar{a}^1) \leq o(a)$

$\Rightarrow \quad n \leq m \longrightarrow ①$

Also since $a = (\bar{a}^1)^{-1}$ i.e a is exponent power of $\bar{a}^1$ so

order of $(\bar{a}^1) \leq o(\bar{a}^1)$

$m \leq n \longrightarrow ②$

By ① & ② we have

$m = n$

(iv) Let $o(a) = n$ and $a^m = e$

$\Rightarrow a^n = e$

Let $n \nmid m$ but

$m = nq + r \quad 0 \leq r < n$

Now $a^m = e$

$a^{nq+r} = e$

$(a^n)^q \cdot a^r = e$

$a^r = e$

$\because 0 \leq r < n$ and n is order of a

$\therefore \quad r = 0$

Hence $m = nq$

$\Rightarrow n \mid q$

(v) Given $o(a) = n$ and $k \mid n$

$\Rightarrow a^n = e \quad n = kq + 0$

$\Rightarrow a^{kq+0} = e$

Theorem: If a, b are two elements of a group G and $ba = a^m b^n$ if $a, b \in G$, then prove that elements $a^m b^{n-2}$, $a^{m-2} b^n$ and ab^{-1} have same order.

Proof:- We have

$$(a^{-1}b)^{-1} = b^{-1}(a^{-1})^{-1} = b^{-1}a$$

Since $b^{-1}a$ is inverse of $a^{-1}b$

$$\therefore \quad o(b^{-1}a) = o(a^{-1}b)$$

Now

$$a^m b^{n-2} = a^m b^n b^{-2} = (ba)b^{-2} \quad \because ba = a^m b^n$$
$$= b(ab^{-1})b^{-1} \quad \because b^{-2} = b^{-1}b^{-1}$$

But $b(ab^{-1})b^{-1}$ has the same order as that of ab^{-1} since.

$$[b(ab^{-1})b^{-2}]^2 = [b(ab^{-1})b^{-1}][b(ab^{-1})b^{-1}]$$
$$= [b(ab^{-1})](b^{-1}b)[(ab^{-1})b^{-1}]$$
$$= b(ab^{-1})^2 b^{-1}$$

or in general

$$[b(ab^{-1})b^{-1}]^n = b(ab^{-1})^n b^{-1}$$
$$= beb^{-1} = bb^{-1} \quad \text{if order of } ab^{-1} = n$$
$$= e.$$

$$\Rightarrow o(ab^{-1}) = o(a^m b^{n-2})$$

Again $a^{m-2}b^n = a^{-2}(a^m b^n) = a^{-2}(ba) = a^{-1}(a^{-1}b)a$

i.e as above $o(a^{-1}b) = o(a^{m-2}b^n)$

Theorem: If the elements a, b and ab of gp G are each of order 2, then show that the gp. is abelian.

Proof:-

$$\because \quad o(ab) = 2$$
$$\therefore \quad (ab)^2 = e, \text{ } e \text{ being identity in } G$$
$$\Rightarrow (ab)(ab) = e$$
$$\Rightarrow a(ab)(ab) = ae = a$$
$$a(ab)(ab)b = ab$$

$$(aa)(ba)(bb) = ab$$
$$(aa)(ba)b^2 = ab$$
$$(aa)(ba)e = ab$$
$$a^2(ba) = ab$$
$$e(ba) = ab$$
$$ba = ab$$

$\Rightarrow$ G is abelian gp

Theorem: Let G be a gp. and $a \in G$, then prove that $\bar{a}^m = (\bar{a}^1)^m$, where m is positive integer.

Proof: We have

$$\bar{a} = \underbrace{(a \cdot a \cdot a \cdot a \cdot a)}_{m \text{ times}}^{-1} = \underbrace{\bar{a}^1 \cdot \bar{a}^1 \cdot \bar{a}^1 \cdot \bar{a}^1 \cdots \bar{a}^1}_{m \text{ times}}$$

$$(a^m)^{-1} = (\bar{a}^1)^m$$

Thus $\bar{a}^m = (\bar{a}^1)^m$

Complexes & Subgroups

Complex Any subset of of a gp. G is called complex in G.

Subgroup

A subset H of a gp G is called sub-gp iff H is itself gp. under the same binary operation as defined in G.

OR

A non-empty subset H of gp G is called subgp of G if the binary operation in G induces a binary operation in H (i.e H is stable for composition in G) and the H. obeys gp axioms.

Remark: Every gp. has at least two subgps., one consisting of identity e alone (unit, identity or trivial) and other G itself. These two subgroups are called improper subgroups

Proper Subgroup A sbgp of G different from identity subgp. and G itself is called proper subgp. of G.

Examples

1: The additive gp of integers is a subgp of the additive group of rational numbers.

2: The multiplicative gp of +ve rational numbers $(\mathbb{Q}^+, \cdot)$ is subgp of the multiplicative gp of non-zero real numbers i.e $(\mathbb{R}^+, \cdot)$

3: $(\mathbb{Q}, +)$ is sub gp of $(\mathbb{R}, +)$ and $(\mathbb{R}, +)$ is subgp of $(\mathbb{C}, +)$

4) The set E of all even integers is a subgp of $(\mathbb{Z}, +)$

4: Set $H_3 = \{3k \mid k \in \mathbb{Z}\}$ and in general $H_n = \{nk \mid k \in \mathbb{Z}\}$

is subgroup of $(\mathbb{Q}, +)$.

If H is subgp of G we write $H \subseteq G$.

Theorem: (i) The identity of subgp is same as that of the group

(ii): The inverse of an element of a subgroup of group is the same as the inverse of the same element regarded as an element of the gp.

Proof: (i) Let H be subgp of a gp. G and let e, e' be identities of G & H respectively. Then

$$ae' = a \quad \forall a \in H$$

This equality will also hold in G as $a \in H \Rightarrow a \in G$

Now if b be the inverse of $a \in G$, then

$$ae' = a$$

$$\Rightarrow bae' = b(ae') = (ba)e' = ba$$

$$\Rightarrow b(ee') = ba \quad ba = e \text{ in } G$$

$$(ba)e' = ba$$

$$ee' = e$$

$$e' = e$$

OR

$ba = e$ in G

$b(ae') = e$

$(ba)e' = e$

$ee' = e \Rightarrow e' = e$.

(ii) Let H be subgroup of the group G and let b_1 & b_2 be the inverses of an element a as member of H and G respectively. If e & e' are identities of G & H, Then $e = e'$

Now

$$ab_1 = e' = e$$

$$\Rightarrow b_2(ab_1) = b_2 e$$

$$(b_2 a)b_1 = b_2$$

$$eb_1 = b_2 \qquad b_2 a = e$$

$$\Rightarrow b_1 = b_2$$

Criterion for a Complex be a sub-group

Theorem:- A non-empty subset H of a gp G is subgroup iff $a, b \in H \Rightarrow ab^{-1} \in H$.

OR

Necessary & sufficient condition for a non-empty Complex H of a group G t.be subgroup is that $a \in H, b \in H \Rightarrow ab^{-1} \in H$.

Proof: Necessary Condition

Let H be a subgroup of G, then H is itself a group under the same binary operation as defined in G.

Let $a, b \in H$

$\because H$ is subgroup

$\therefore b \in H \Rightarrow b^{-1} \in H$.

Hence $a \in H, b^{-1} \in H \Rightarrow ab^{-1} \in H$.

Sufficient Condition

Suppose for each pair $a, b \in H \Rightarrow ab^{-1} \in H$. Then we prove that H is gp under the same binary operation as defined in G.

(I) Since H is non-empty, $\exists\ a \in H$ and $a\bar{a}^{-1} \in H \Rightarrow e \in H$. So H Contains identity

(II) Let $b \in H$. As $e \in H$, $eb^{-1} = b^{-1} \in H$

Hence $b \in H \Rightarrow b^{-1} \in H$.

$\therefore$ Inverse of every element of H is present in H.

III $a, b \in H$

$\Rightarrow a, b^{-1} \in H$

$\Rightarrow a(b^{-1})^{-1} \in H \Rightarrow ab \in H$.

So H is closed under the binary operation

IV Also associative law holds in H because it holds in G

Note The condition

$a \in H, b \in H \Rightarrow ab^{-1} \in H$

may also be expressed by the statement $HH^{-1} \subseteq H$

Theorem:- A subset H of a group G is a subgp. iff for any pair $a, b \in H$, $ab \in H$ and for each $a \in H$, $a^{-1} \in H$.

Proof:- Suppose H is a subgp of G, then H is closed under multiplication of G

so $a, b \in H \Rightarrow ab \in H$ (Closure property of gp)

Also for each $a \in H$, $a^{-1} \in H$ ($\because H$ is gp)

Conversely, for $a, b \in H$, $ab \in H$ and for $a \in H$, $a^{-1} \in H$

Then

$$a, b \in H \Rightarrow a, b^{-1} \in H \quad (\because a \in H \Rightarrow a^{-1} \in H)$$
$$\Rightarrow ab^{-1} \in H \quad (\because a, b \in H \Rightarrow ab \in H)$$

Hence H is subgroup of G.

Example: Let $(\mathbb{Z}, +)$ be the group of integers, under addition and E be the set of even integers, we show that E is subgroup of G.

Solution: Let $a, b \in E$

$$\Rightarrow a = 2m, \; b = 2n \quad \forall m, n \in \mathbb{Z}$$

Then $a - b = 2(m - n) \in E$

Hence $(E, +)$ is subgroup of G.

Theorem:- (Special case of finite groups)

A necessary and sufficient condition for a Complex H of a finite group G to be sub-gp is that

$$a \in H, \; b \in H \Rightarrow ab \in H$$

Proof:- Necessary Condition

Let H be subgroup of a finite gp G and $a, b \in H$. Then $ab \in H$

Sufficient Condition

Let $a \in H$. The group being finite, the order of a is finite, say n. Then $a^n = e$

$\because$ For $a, b \in H$, $ab \in H$

By successive applications of the criterion

$$a \in H \Rightarrow a^n = e \in H \Rightarrow a^{n-1} = a^{-1} \in H$$
$$(\because a^{n-1} \in H)$$

Now since for $a, b \in H$, $ab \in H$ & $a \in H \Rightarrow a^{-1} \in H$
Hence H is subgroup

Note Here $a^n = e$

Now $a^n = \underbrace{a.a.a.a.a \cdots a}_{n \text{ times}}$

Here $a.a \in H$

$\Rightarrow (a.a)a \in H$

$\Rightarrow (a.aa)a \in H$

$\Rightarrow \underbrace{a.a.a.a \cdots a}_{n-1 \text{ times}} \in H$

$\Rightarrow \underbrace{a.a.a.a \cdots a}_{n \text{ times}} \in H$

$\Rightarrow a^n \in H \Rightarrow e \in H$

$a^n \in H$
$\Rightarrow a^{n-1}.a \in H$

Now $a^n = e \Rightarrow a^{n-1} = a^{-1}$

But $a^{n-1} \in H \Rightarrow a^{-1} \in H$.

Another form

A necessary and sufficient condition for a complex H of a finite group G to be a sub group thereof is that

$$HH = H$$

Proof :- (M)

Let H be a subgroup of finite gp G. Then

for $a, b \in H \Rightarrow ab \in H$

But for $a, b \in H$, $ab \in HH$

$\Rightarrow ab \in HH \Rightarrow ab \in H$

$\Rightarrow HH \subseteq H$ ——— (1)

Again Let $a \in H$

$\because H$ is subgp, $e \in H$

$\Rightarrow ae = a \in HH$

$\Rightarrow H \subseteq HH$ ——— (2)

By (1) & (2) $H = HH$.

$KL = \{xy : x \in K, y \in L\}$

Conversely for any subset H of a finite gp G.
$HH = H$
Then for $a, b \in H$, $ab \in H$ ($\because HH = H$)
Also since H is finite
$\therefore$ order of $a \in H$ is finite say, n i.e
$a^n = e$.
$\Rightarrow$ $(\underbrace{a \cdot a \cdot a \cdot a \cdot a \cdot a \cdots a}_{n-1 \text{ times}}) a \in H$ ($\because ab \in H, ab \in H$)
$\Rightarrow a^n \in H$.
$\Rightarrow \underbrace{a \cdots a \cdot a \cdot \cdots a}_{n-1 \text{ times}} \in H$
$a^{n-1} \in H$.
but $a^n = e \Rightarrow a^{n-1} = a^{-1}$
$\Rightarrow a^{-1} \in H$
Hence H is subgroup of G.

Theorem The intersection of any two subgroups of a gp G is again subgroup of G.

Proof:- Let H_1 & H_2 be two subgroup of gp G
Since $e \in H_1 \cap H_2$, $H_1 \cap H_2 \neq \phi$ (non-empty)
Now $a, b \in H_1 \cap H_2 \Rightarrow a, b \in H_1$ and $a, b \in H_2$
$\Rightarrow ab^{-1} \in H_1$ & $ab^{-1} \in H_2$
$\Rightarrow ab^{-1} \in H_1 \cap H_2$
Hence $H_1 \cap H_2$ is a subgp of gp G.

Remark It may be noted that $H_1 \cap H_2$ is the largest subgroup contained in H_1 and H_2

Theorem: The intersection of any arbitrary family of subgroups is a subgroup.
Proof: Let $\{A_\alpha : \alpha \in \Lambda\}$ be any collection of subgroups of a group G and
Let $H = \bigcap_{\alpha \in \Lambda} A_\alpha$

Then we show that H is a subgroup of G.

Let $a, b \in H$

$\Rightarrow a, b \in \bigcap_{\alpha \in \Omega} A_\alpha$

$\Rightarrow a, b \in A_\alpha \quad \forall \alpha \in \Omega$

Since each A_α is a subgp.

$\therefore a, b \in A_\alpha \Rightarrow ab^{-1} \in A_\alpha \quad \forall \alpha \in \Omega$.

$\Rightarrow ab^{-1} \in \bigcap_{\alpha \in \Omega} A_\alpha$

$\Rightarrow ab^{-1} \in H$

So H is a subgroup of G.

Remark :- Intersection of a collection of subgroups of a group G is obviously the largest subgp contained in every member of the collection.

Theorem The union of two subgroups of a gp G may not be a subgroup.

Proof :- Let H_1 & H_2 be the two subgroups of gp G. and let $a \in H_1$, $b \in H_2$

$\Rightarrow a, b \in H_1 \cup H_2$.

Now $a, b \in H_1 \cup H_2 \Rightarrow a \in H_1, b \in H_2 \Rightarrow ab \in H_1 \cup H_2$, for may not belong to H_1

Hence union of two subgps may not be subgp.

See example

Theorem :- The union of two sub-groups is a sub-group is a sub-group iff one is contained in other. OR

The union $H \cup K$ of two sub-groups H & K of a group G is a sub-group of G iff $H \subseteq K$ or $K \subseteq H$.

Proof :- Suppose H & K are sub-groups of a group G, and also suppose $H \subseteq K$ or $K \subseteq H$.

Then

$H \cup K = H$ or K. So $H \cup K$ is subgp of G.

Conversely suppose that for two sub-groups H & K of G, HUK is sub-group of G and

$$H \not\subseteq K, \quad K \not\subseteq H$$

Then there are elements $a \in H, b \in K$ s.t. $a \notin K, b \notin H$

Now $a, b \in HUK$, where HUK is sub-group

so $ab \in HUK$

Thus $ab \in H$ or $ab \in K$

If $ab \in H$, then

$b = a^{-1}(ab) \in H$ ($\because H$ is sub-group)

which is a contradiction because $b \notin H$

Similarly if $ab \in K \Rightarrow a = (ab)b^{-1} \in K$

which is a contradiction because $a \notin K$

Thus either $H \subseteq K$ or $K \subseteq H$

Theorem Let A be an abelian group. Then the set P consisting of those elements of A which have finite order is a sub-group of A.

Proof:-

Let $a, b \in P$. Then there exist integers m and n such that

$$a^m = e \qquad b^n = e$$

$$(ab)^{mn} = a^{mn} b^{mn}$$

so $(b^{-1})^n = (b)^{-n} = (b^n)^{-1} = e^{-1} = e$

$\Rightarrow$ b^{-1} has finite order and will belong to P

$\therefore$ ab^{-1} also has finite order

$\therefore$ $ab^{-1} \in P$

$\Rightarrow$ P is a sub-group of A

Note: (1) Such subgroup is called periodic part of A.

(2) A group whose all elements have finite order is called periodic group

57 **Homomorphism**

Let $(G, \cdot)$ & $(G', \times)$ be two groups. A mapping $\varphi: G \longrightarrow G'$ is called homomorphism of G to G' if for every pair $a, b \in G$

$$\varphi(a.b) = \varphi(a) \times \varphi(b)$$

i.e image of product in G is equal to the product of images in G'.

Remark: (i) If G is homomorphic to G', then there may exist more than one homorphism of G into G'.

(ii) Homomorphic mapping may be many one.

(iii) The relation of homomorphism is not symmetric. i.e If G is homomorphic to G', G' may not be homomorphic to G.

(iv) Homomorphism retains/preserves the structure

Properties of Homomorphism:

Theorem: If $\varphi: G \longrightarrow G'$ is homomorphism, then

(i) The homomorphic image of the identity of G is the identity of G' i.e.

$$\varphi(e) = e' \quad \text{where } e, e' \text{ are identities of } G \text{ \& } G' \text{ respectively.}$$

ii): The homomorphic image of the inverse of any element 'a' of G is the inverse of the image of a.

iii) The order of the homomorphic image of an element (a) is a divisor of the order of a

(iv) The image of a power of an element of G is power of image of that element. i.e $\varphi(a^m) = [\varphi(a)]^m$

Proof:-

(i) Let $a \in G \Rightarrow \varphi(a) \in G'$

and $\varphi(a.e) = \varphi(a) \times \varphi(e) \quad \forall\, a \in G$

$\therefore \varphi(a) \times e' = \varphi(a) = \varphi(a.e) = \varphi(a) \times \varphi(e)$

$\Rightarrow e' = \varphi(e)$ left cancellation law.

(iv) Let $a \in G$

$\varphi(a^m) = \varphi(\underbrace{a \cdot a \cdot a \cdots a}_{m \text{ times}}) = \underbrace{\varphi(a) \times \varphi(a) \times \cdots \times \varphi(a)}_{m \text{ times}}$

$= [\varphi(a)]^m$

SB

ii) $\because a, \bar{a}^{-1} \in G \Rightarrow \varphi(a), \varphi(\bar{a}^{-1}) \in G'$

$\therefore \varphi(a) \times \varphi(\bar{a}^{-1}) = \varphi(a \cdot \bar{a}^{-1}) = \varphi(e) = e'$

$\Rightarrow [\varphi(a)]^{-1} = \varphi(\bar{a}^{-1})$

iii) (myself) Let $o(a) = n$ $\quad o(\varphi(a)) = m$

$\Rightarrow a^n = e$ $\quad [\varphi(a)]^m = e'$

Let $n = mq + r$ $\quad 0 \le r < m$.

Then $a^n = e \Rightarrow \varphi(a^n) = \varphi(e) = e'$

$\Rightarrow [\varphi(a)]^n = e'$

$[\varphi(a)]^{mq+r} = e'$

$[\varphi(a)]^r = e'$ but $o \le r < m$

$\Rightarrow r = 0$ Hence m/n

Examples of Homomorphism

Example 1: Let $(Z, +)$ be the group of integers under addition and $G_1 = \{2^n : n \in Z\}$ is gp under usual multiplication of real numbers.

Define $f : Z \longrightarrow G_1$ by

$f(n) = 2^n \quad \forall n \in Z$

Then

$f(n+m) = 2^{n+m} = 2^n \cdot 2^m \quad \forall n, m \in Z$

$= f(n) \cdot f(m)$

$\Rightarrow f$ is a homomorphism of Z into G_1.

Clearly f is onto and G_1 is a homomorphic image of Z.

Example 2: Let G_1 be the multiplicative gp. of all $n \times n$ singular matrices over the real numbers. Let R^* be the multiplicative gp of all non-zero real numbers.

Define $f : G_1 \longrightarrow R^*$ by

$f(A) = \det A$ i.e. $|A|$

$\because$

$f(AB) = \det(AB) = \det(A) \cdot \det(B)$

$= |A||B|$

$\Rightarrow$ f is homomorphism of G into R^*. f is also onto because every det is image of some $(n \times n)$ matrix.

Example: 3: Let $G = \{1, -1\}$, G is a group under multiplication.

Define $f: Z \longrightarrow G$ as

$f(n) = 1$ if n is even.

$f(n) = -1$ if n is odd

Let $a, b \in Z$

following cases arise.

Case I: Both m, n are even. Then $m+n$ is even.

$f(m) = 1 \quad f(n) = 1$

$\Rightarrow f(m+n) = 1 = 1 \cdot 1 = f(m) \cdot f(n)$

$\Rightarrow f$ is homomorphism.

Case II:- One of m and n is even and other is odd. Let m is even and n is odd

$f(m) = 1 \quad f(n) = -1$

Also $m+n$ is odd

$\Rightarrow f(m+n) = -1 = 1(-1) = f(m) \cdot f(n)$

Case III: Both m and n are odd. Then

$f(m) = -1$ and $f(n) = -1$

Now $m+n$ is even

$\Rightarrow f(m+n) = 1 = 1 \cdot 1 = f(m) \cdot f(n)$

Thus $f(m+n) = f(m) \cdot f(n) \quad \forall\, m, n \in Z$

Since $f(2) = 1$, $f(3) = -1$

$\therefore$ f is onto. Hence f is epimorphism; consequently G is homomorphic image of Z

Example: 4: Let $(Z, +)$ be the group of integers under addition. and $Z_2 = \{0, 1\}$ be the gp of integers under addition modulo 2

Define a mapping as follows

$\alpha(n) = 0$ if n is even

$= 1$ if n is odd.

α is obviously surjective.

For $m, n \in Z$, we have following cases.

Case-I:- Both m, n are even

In this case $m+n$ is even and

$\alpha(m+n) = 0 = 0+0 = \alpha(m)+\alpha(n)$

Case-II: When one of m, n is even and the other is odd. Let m is even and n is odd. Then $(m+n)$ is odd. So

$\alpha(m+n) = 1 \pmod 2$

$= 0+1 = \alpha(m)+\alpha(n)$

Case-III: When both m & n are odd, then $m+n$ is even

$\alpha(m+n) = 0 = 1+1 \pmod 2$

$= \alpha(m)+\alpha(n)$

Hence $\alpha(m+n) = \alpha(m)+\alpha(n)$ $\forall m, n \in Z$.

Thus α is epimorphism.

Example:5:- Let $(R^+, \cdot)$ be the gp of all non-zero real nos. under multiplication and $(R, +)$ be the group of all real numbers under addition.

Define a mapping $\varphi: R^+ \longrightarrow R$ as

$\varphi(x) = \log(x)$ $\forall x \in R^+$.

Then

$\varphi(x \cdot y) = \log(x \cdot y) = \log x + \log y$

$= \varphi(x) + \varphi(y)$

Therefore φ is homomorphism.

Example:6: Let $(R^+, +)$ and $(R, \cdot)$ be groups.

Define mapping $\psi: R^+ \longrightarrow R$ as

$\psi(x) = e^x$ $\forall x \in R^+$

Then for $x, y \in R^+$

$\psi(x+y) = e^{x+y} = \psi(x) \cdot \psi(y)$

Therefore ψ is a homomorphism.

Epi- morphism:

A homomorphism $\varphi: G \longrightarrow G'$, which is at the same time onto (Surjective) is called epic or epi-morphism.

Mono- morphism: or **Monic**

A homomorphism $\varphi: G \longrightarrow G'$ is called a monomorphism if φ is injective (one-one)

OR

Let $(G, \cdot)$ & $(G', *)$ be two groups. A mapping $\varphi: G \longrightarrow G'$ is said to be monomorphism if

(i) φ is homomorphism

(ii) φ is one-one (Injective)

Example: Mapping $\psi: R \longrightarrow R^+$ defined by

$\psi(x) = e^x$ is monomorphism.

Here for $x, y \in R$.

$$\psi(x) = \psi(y)$$
$$\Rightarrow e^x = e^y$$
$$e^x \cdot \bar{e}^y = 1 = e^0$$
$$\Rightarrow x - y = 0 \Rightarrow x = y$$

Endo- morphism:

A homomorphism of a gp G into itself is called an endomorphism of G

OR

A homomorphism $\varphi: G \longrightarrow G$ is called endo-morpheism.

Examples-

(i) Let $(Z, +)$ be the set of integers under addition. Define a mapping $\varphi: Z \longrightarrow Z$ as

$\varphi(n) = 2n \quad \forall n \in Z$

Then $\forall m, n \in Z$

$$\varphi(m+n) = 2(m+n)$$
$$= 2m+2n$$
$$= \varphi(m) + \varphi(n)$$

So φ is endo-morphism.

In general for any integer k the mapping $\varphi_k : Z \to Z$ defined by

$$\varphi_k(n) = (k+1)n \quad \forall n \in Z$$

is a endo-morphism

(ii) For any group G, the mapping $I: G \to G$ defined by

$$I(x) = x \quad \forall x \in G$$

is an endo-morphism

$$I(x \cdot y) = xy = I(x) \cdot I(y)$$

Homomorphic Image

If $\varphi : G \to G'$ is a homomorphism, then the set $\varphi(G)$ is called the homomorphic image of $(G,$ under φ: If φ is epic, then homomorphic image of G under φ is G'.

Theorem: Let $\varphi : G \to G'$ be a given homomorphism from $(G, \cdot)$ to $(G', \times)$, then $\varphi(G)$ is a subgroup of G'

Proof: Let $x, y \in \varphi(G)$

Then $\exists\ a, b \in G$ such that

$$\varphi(a) = x \qquad \varphi(b) = y$$

$$\varphi(ab^{-1}) = \varphi(a) \times \varphi(b^{-1}) \quad (\because \varphi \text{ is homo.})$$
$$= \varphi(a) \times [\varphi(b)]^{-1}$$
$$= x \times y^{-1} = x \times y^{-1}$$

$\because G$ is group $\therefore ab^{-1} \in G$

Hence $x \times y^{-1} \in \varphi(G)$

Thus $\phi(G)$ is sub-group of G'

Kernel of a Homomorphism

If ϕ is homomorphism of G into G', then the kernel subset of those elements of G which are mapped onto the identity of G' under ϕ is called kernel of ϕ and is denoted by $\ker(\phi)$ or $\phi^{-1}(e')$. Thus

$$\phi^{-1}(e') = \ker(\phi) = \{x : x \in G \text{ and } \phi(x) = e'\}$$

Theorem (properties relating to kernel)

If f is a homomorphism into G', then

(i) $\ker f$ is sub-group (normal) of G

(ii) Homomorphism f is a monomorphism iff $\ker(f) = \{e\}$

Proof:

$$\ker(f) = \{f^{-1}\{e'\}\} = \{x \in G : f(x) = e'\}$$

Since $f(e) = e'$ (f is homomorphism)

$\Rightarrow \ker f \neq \phi$

Let $a, b \in \ker(f)$

$\Rightarrow f(a) = e' = f(b)$

We have

$$f(ab^{-1}) = f(a) \cdot f(b^{-1}) = f(a)[f(b)]^{-1} = e' \cdot e'^{-1} = e' \cdot e' = e'$$

$\Rightarrow ab^{-1} \in \ker f$

$\Rightarrow \ker(f)$ is a sub-gp of G.

OR

(a) Closure Law: Let $a, b \in \ker(f)$

$\Rightarrow f(a) = e' = f(b)$

$f(ab) = f(a) \cdot f(b) = e' \cdot e' = e'$

$\Rightarrow ab \in \ker(f)$ i.e closure law holds

(b) Associative Law: Since $\ker(f)$ is subset of G, associative law is self-evident.

(c) Identity: $\because f(e) = e' \Rightarrow e \in \ker(f)$
$\therefore$ There exists identity in $\ker(f)$

(d) Inverse Let $a \in \ker(f)$
Then $f(\bar{a}') = [f(a)]^{-1} = (e')^{-1} = e'$
$\Rightarrow \bar{a}' \in \ker(f)$
Hence $\ker(f)$ is sub-group of G.

(ii) Let f be 1-1, $x \in \ker(f)$. Then
$f(x) = e' \Rightarrow x = e$ ($\because f$ is 1-1)
This proves that $\ker(f) = \{e\}$
Conversely let $\ker(f) = \{e\}$
Let $x, y \in G$, be such that $f(x) = f(y)$
Then $f(x\bar{y}') = f(x) f(\bar{y}') = f(x)[f(y)]^{-1} = e'$
$\Rightarrow x\bar{y}' \in \ker(f) = \{e\}$
$\Rightarrow x\bar{y}' = e \Rightarrow x = y$
Hence f is 1-1

Isomorphism

Let G & G' be two groups. Then a mapping $\varphi: G \longrightarrow G'$ is called isomorphism if
(i) φ is homomorphism
(ii) φ is bijective (1-1 & onto)

OR

A homomorphism $\varphi: G \longrightarrow G'$ which is simultaneously an epimorphism and a monomorphism is called isomorphism.

Examples

1: Mappings $\varphi: R^+ \longrightarrow R$ and $\psi: R \longrightarrow R^+$ defined by
$\varphi(x) = \log x \quad \forall x \in R^+$
$\psi(x) = e^x \quad \forall x \in R$
respectively are isomorphisms.

Note Prove how $\varphi: R^+ \longrightarrow R$ is surjective.
Set $y \in R$, then $e^y \in R^+$
and $\varphi(e^y) = \log(e^y) = y$
$\Rightarrow \varphi$ is surjective.

Q: Let Z be the group of integers under addition and E be the group of even integers under addition. Define a mapping $\varphi: Z \longrightarrow E$ by

$$\varphi(n) = 2n \qquad \forall n \in Z$$

Then φ is homomorphism because for $x, y \in Z$

$$\varphi(x+y) = 2(x+y)$$
$$= 2x + 2y$$
$$= \varphi(x) + \varphi(y)$$

φ is 1–1 because.

$$\varphi(m) = \varphi(n)$$
$$\Rightarrow 2m = 2n$$
$$\Rightarrow m = n$$

φ is onto because each $2n \in E$ is the image of $n \in Z$

Thus φ is isomorphism.

Properties of Isomorphism

Theorem Let f be an isomorphism of G_1 onto G'. Then

(i): The order of G_1 = the order of G'

(ii) The image of identity of G_1 is the identity of G' i.e $f(e)$ is the identity of G'

(iii) The image of inverse of any element 'a' of G_1 is the inverse of the image of 'a' i.e.

$$f(a^{-1}) = [f(a)]^{-1}$$

(iv) The order of an element is same as the order of the image of the element i-e order of an element is invariant for isomorphic mappings

(v) f^{-1} is also isomorphic

Proof:-

(i) Since f is one-one onto

$\therefore \quad O(G) = O(G')$

(ii) Let for any $a \in G$ $\exists$ an element $a' \in G'$ such that

$$f(a) = a'$$

Now $ae = a$

$\Rightarrow f(ae) = f(a)$

$\Rightarrow f(a) f(e) = f(a)$ ($\because f$ is homo-morphism)

$\Rightarrow a' f(e) = f(a)$

$\Rightarrow a' f(e) = a'$

$\Rightarrow a' f(e) = a'e'$

$f(e) = e'$ (by left cancellation law)

Similarly by $ea = a$ we have

$f(e)a' = ea'$

$\Rightarrow f(e) = e$ (Right cancellation law)

(iii) $f(e) = e'$

Also $\bar{a}'a = e = a\bar{a}'$

$a\bar{a}' = e \Rightarrow f(a\bar{a}') = f(a) f(\bar{a}') = f(e)$

$\bar{a}'a = e \Rightarrow f(\bar{a}') f(a) = f(e)$ $\Big\} \Rightarrow [f(a)]^{-1} = f(\bar{a}')$

(iv) Let n be the order of an element $a \in G$ and m be the order of $f(a)$. Then

$a^n = e$ & $[f(a)]^m = e'$

But $a^n = e$

$\Rightarrow f(a^n) = f(e)$

$\Rightarrow f(a \cdot a\ a \cdots n \text{ times}) = e'$

$\Rightarrow f(a) f(a) \cdots f(a) \cdots n \text{ times} = e'$

$\Rightarrow [f(a)]^n = e'$

$\Rightarrow$ order of $f(a) \leq n$

Also $\Rightarrow m \leq n \longrightarrow ①$

$[f(a)]^m = e'$

$\Rightarrow f(a)\, f(a) \ldots\ldots m \text{ times} = f(e)$

$\Rightarrow f(a.a\,a\,a \ldots\ldots m \text{ times}) = f(e)$ by definition of isomorphism

$\Rightarrow f(a^m) = f(e)$

$\Rightarrow a^m = e$ $\because f$ is one-one

$\Rightarrow$ order of $a \leq m$

$\Rightarrow n \leq m \longrightarrow ②$

By ① & ② $m = n$

$\therefore o(a) = o(f(a))$

OR

Let order of a, be finite m so that

$a^m = e$

$\Rightarrow [f(a)]^m = f(e)$

$\Rightarrow$ The order of $f(a) \leq m$

If now the order of $f(a)$ is $k < m$

Then $[f(a)]^k = f(e)$

$\Rightarrow f(a^k) = f(e)$

$\Rightarrow a^k = e$

which is a contradiction.

Hence $a^k \neq e$ and $k \geq m$

It can be shown that if the order of a is infinite, then the order of $f(a)$ is also infinite.

Let order of 'a' is infinite i.e there does not exist +ve integer m such that

$a^m = e$

- Suppose that order of $f(a)$ is finite and is n such that

$$[f(a)]^n = f(e)$$

$$f(a^n) = f(e)$$

$$\Rightarrow a^n = e.$$

$\Rightarrow$ order of $a \leq n$ i.e finite.

which is a contradiction because order of a is infinite

Thus $o(f(a)) =$ infinite.

(V)

Since f is one-one and onto

$\therefore f^{-1}$ exists and is also one-one onto

Also if

$x = f(a)$ $y = f(b)$ for $a, b \in G$ & $x, y \in G'$

Then

$$a = f^{-1}(x) \quad , b = f^{-1}(y)$$

$$f^{-1}(xy) = f^{-1}[f(a)\, f(b)]$$

$$= f^{-1}(f(ab)) = ab$$

$$= f^{-1}(x)\, f^{-1}(y)$$

$\Rightarrow f^{-1}$ retains the group structure and hence f^{-1} is isomorphism.

Theorem: The relation of isomorphism in the collection (set) of all groups is an equivalence relation:

Proof: Let C be the class of all groups. Define a relation R on C as follows. For $G_1, G_2 \in C$, we say $G R G'$ if there is an isomorphism $\varphi: G \to G'$. We show R is an equivalence relation.

(a) Reflexivity:- Define a mapping $I: G \longrightarrow G$ by

$$I(x) = x \quad \forall x \in G$$

Then obviously I is one-one and onto

Moreover

$$I(xy) = xy = I(x).I(y)$$

$\Rightarrow$ I is an isomorphism

$\Rightarrow$ $G \cong G$ i.e $G R G$

$\Rightarrow$ Relation of isomorphism is reflexive.

(b) Symmetry: Suppose that $G \cong G'$, then $\exists$ an isomorphism $\phi: G \longrightarrow G'$

Since ϕ is bijective, mapping $\bar{\phi}^1: G' \longrightarrow G$ given by

$$\bar{\phi}^1(y) = x \quad \text{if } f(x) = y \quad \forall y \in G'$$

is also bijective.

Also let $g_1', g_2' \in G'$.

Since ϕ is bijective we can find $g_1, g_2 \in G$ such that

$$\bar{\phi}^1(g_1') = g_1 \;,\; \bar{\phi}^1(g_2') = g_2$$

so

$$\begin{aligned}
\bar{\phi}^1(g_1' g_2') &= \bar{\phi}^1(\phi(g_1)\,\phi(g_2)) \\
&= \bar{\phi}^1(\phi(g_1 g_2)) \qquad \because \phi \text{ is homomorphism} \\
&= \bar{\phi}^1 \phi(g_1 g_2) = I(g_1 g_2) \\
&= g_1 g_2 \\
&= \bar{\phi}^1(g_1')\,\bar{\phi}^1(g_2')
\end{aligned}$$

Hence $\bar{\phi}^1$ is an isomorphism and so $G' \cong G$ i.e $G' R G$

Transitivity: Let, for $G', G'', G''' \in C$ $G R G'$, $G' R G'''$ i.e.

$G \cong G'$ and $G' \cong G'''$

$\Rightarrow$ $\exists$ isomorphism $\phi: G \longrightarrow G'$ and $\psi: G' \longrightarrow G''$.
Since ϕ & ψ are bijective mappings, $\psi\phi$ from G to G''' is also bijective
Also for $g_1, g_2 \in G$

$$(\psi\phi)(g_1 g_2) = \psi(\phi(g_1 g_2))$$
$$= \psi(\phi(g_1)\phi(g_2))$$
$$= \psi(g_1' g_2')$$
$$= \psi(g_1')\psi(g_2')$$
$$= \psi(\phi(g_1))\psi(\phi(g_2))$$

Hence $\psi\phi$ is an isomorphism.
so $G R G'''$
Hence relation of isomorphism is an equivalence relation.

Remarks

(i) Composite of two homomorphisms is again a homomorphism.
(ii) If $G_1 \cong G_2$ and f is underlying isomorphism of G_1 onto G_2, then for any $x, y \in G$, $xy = z$ $\Rightarrow$ $f(x)f(y) = f(z)$. This means if f is known, x and y are known, then $f(x), f(y)$ being equal to $f(xy)$ is known in G_2, the moment xy is known in G_1. Similarly if we know the binary Composition g of G_2 to G_1, which is an isomorphism. then the binary composition on G_1 is know completely. Thus if all the properties of the G_1 which are dependent on its binary composition are known, then all the properties of the other which depend upon its binary composition are also known.

Because of these reasons two isomorphic groups can be regarded to be identical

Problem If R^* is the group of non-zero real numbers under multiplication, then show that $(R^*, \cdot)$ is not isomorphic to $(R, +)$

Solution: $-1 \in R^*$ is of order 2. So if $(R^*, \cdot) \cong (R, +)$ say, under an isomorphism f; then $f(-1)$ must be of order two. But for every $a \in R$, $na = 0 \Rightarrow n = 0$ or $a = 0$. So there is no element of order 2 in $(R, +)$. Hence $(R^*, \cdot)$ can not be isomorphic to $(R, +)$

Problem: For any homomorphism $f: G \to H$ prove that, if $x \in G$ is of finite order, then $o(f(x)) \mid o(x)$ and conclude that f is a monomorphism if and only if $o(x) = [o(f(x))]\ \forall x \in G$.

Solution:

Let x be of finite order say, m i.e $x^m = e$.

$\Rightarrow f(x^m) = f(e)$

$[f(x)]^m = f(e)$

$\Rightarrow$ order of $f(x) \leq m$

Let order of $f(x)$ be k such that $k \leq m$ and suppose that $k \nmid m$. Then

$m = kq + r \quad 0 < r < k$

Now

$[f(x)]^m = f(e)$

$\Rightarrow [f(x)]^{kq+r} = f(e)$

$([f(x)]^k)^q [f(x)]^r = f(e)$

$e^{iK} [f(x)]^r = f(e)$

$$[f(x)]^k = f(e) = e'$$

$\Rightarrow$ order of $f(x) \leq k$

i.e. $k \leq k$

which is a contradiction.

Hence k/m i.e. $o[f(x)]/o(x)$

Now let f is mono-morphism.

Let $x \in G$, of order n i.e.

$$x^n = e$$

$$\Rightarrow f(x^n) = f(e)$$

$$[f(x)]^n = f(e)$$

$$\Rightarrow o(f(x)) \leq n$$

Let order of $f(x)$ be $m < n$. Then

$$[f(x)]^m = f(e)$$

$$f(x^m) = f(e)$$

$\Rightarrow x^m = e$ $\because f$ is one-one.

which is a contradiction because $o(x) = n$

Hence $o(f(x)) = o(x)$

Conversely let $o(f(x)) = o(x)$ $\forall x \in G$,

If $x, y \in G$ such that

$$f(x) = f(y)$$

$$\Rightarrow o(f(x)) = o(f(y))$$

$$\Rightarrow o(x) = o(y)$$

$\Rightarrow$

But $o(f(x)) = o(x) \Rightarrow f$ is isomorphism

$\Rightarrow f$ is one-one.

Problem Prove that if $\theta: F \to G$ and $\phi: G \to F$ are two homomorphisms such that $\theta\phi$ = identity mapping on F and $\phi\theta$ = identity mapping on G, then θ and ϕ are isomorphism of F onto G and of G on F respectively.

Solution:

θ is one-one since

if $\theta(x) = \theta(y)$ $\forall x, y \in F$

Then $x\theta = y\theta$.

$x\theta\phi = y\theta\phi$

$\because$ $\theta\phi$ is identity mapping.

$\therefore$ $x = y$

Similarly ϕ is one-to-one.

Next let $g \in G$, then $g\phi \in F$, $g\phi\theta = g$

Hence g is the image of of an element of F under θ and so θ is an onto mapping.

Thus θ is an isomorphism. Similarly ϕ is an isomorphism.

Theorem (Transference of Group Structures)

If G is a group and G' is a set with a composition (supposed denoted multiplicatively) and there exists a one-one mapping f of G into G' such that

$f(a,b) = f(a)f(b)$ $\forall a, b \in G$

Then G' is also a group isomorphic to G for the composition in question.

Proof We are to show that G' is a gp and $G' \cong G$

(a) **Associativity**: Set $a' = f(a)$ $b' = f(b)$, $c' = f(c)$

: $a, b, c \in G$ and $a', b', c' \in G'$

$$(a'b')c' = [f(a)\,f(b)]\,f(c)$$
$$= [f(ab)]\,f(c)$$
$$= f[(ab)c] = f[a(bc)]$$
$$= f(a)[f(bc)]$$
$$= f(a)\{[f(b)][f(c)]\} = a'(b'c')$$

Identity :- Let e denote the identity of gp G, we have

$$[f(e)]\,a' = [f(e)][f(a)]$$
$$= f(ea) = f(a) = a'$$

Similarly $a'[f(e)] = a'$

Thus $f(e)$ is the identity of G'

Invertibility we have

$$a\bar{a}' = e$$
$$\Rightarrow f(a)\,f(\bar{a}') = f(e)$$
$$a'\,f(\bar{a}') = f(e)$$

Similarly $f(\bar{a}')\,a' = f(e)$

Thus $f(\bar{a}')$ is the inverse of a' in G' i.e.

$$[f(\bar{a}')]^{*} = (a')^{-1} = [f(a)]^{-1}$$

Closure Law :-

$$a, b \in G \Rightarrow f(a), f(b) \in G$$
$$\Rightarrow ab \in G \Rightarrow f(ab) \in G'$$
$$\Rightarrow f(a)\,f(b) \in G'$$
$$\Rightarrow a'b' \in G' \quad \forall\ a', b' \in G$$

Hence G' is a gp and

$$G' \cong G.$$

Embedding of a Group into a Group

An embedding of a group G into a group G' (a more generally, a set G' with an algebric operation) is simply a monomorphism of G into G'.

If G is embedded in a group G' then G' contains a subgp H' isomorphic to G. In general there can be more than one embedding of a gp in a given gp. This simply means that a gp can have more than one isomorphic subgps.

For example group S_A (set of all bijective mappings of a non-empty set A) is gp under usual multiplicaten and in particular the set

$I_A, \phi, \phi^2, \psi, \phi\psi, \phi^2\psi$ of bijective mappings of the set $A = \{a, b, c\}$ is a gp. The mappings ϕ & ψ satisfy the relation

$$\phi^3 = \psi^3 = (\phi\psi)^2 = I_A$$

This gp has three subgroups of order 2 namely the subgroups

$$\{I_A, \psi\}, \{I_A, \phi\psi\} \text{ & } \{I_A, \phi^2\psi\}$$

Theorem: (Cayley's theorem)

Any group G can be embedded in a gp of bijective mappings of a certain set.

OR

Every group is isomorphic to a permutation group (or transformation group)

Proof: Let G be a group. For each $g \in G$, let a mapping $f_g : G \to G$ be defined

by

$$f_g(x) = gx \quad \forall x \in G$$

Then f_g is a bijective mapping because

$$f_g(x) = f_g(y)$$
$$\Rightarrow gx = gy$$
$$\Rightarrow x = y$$

and any element $y \in G$ is the image of $g^{-1}y \in G$ i.e

$$f_g(g^{-1}y) = gg^{-1}y = y$$

Thus f_g is a permutation on set G.

Consider the set

$G' = f_G = \{ f_g : g \in G \}$ of permutations on G.

Let $f_g, f_{g'} \in G'$. Then for any $x \in G$.

$$(f_g \circ f_{g'})(x) = f_g(f_{g'}(x)) = f_g(g'x)$$
$$= gg'x = f_{gg'}(x) \in G'$$

Because composition of bijective mappings is a bijective mapping.

Set G' is a subgroup of the group of all bijective mappings on Set G. because.

For $f_g, f_{g'} \in G'$, $f_g, f_{g'}^{-1} \in G$ and

$f_g \circ f_{g'}^{-1} \in G'$.

We show that G is isomorphic to $G' = f_G$

For this consider a mapping
$\varphi : G \longrightarrow G'$ defined by

$$\varphi(g) = f_g$$

We have

$$\varphi(gg') = f_{gg'} = f_g \circ f_{g'} = \varphi(g) \circ \varphi(g')$$

$\Rightarrow$ φ is a homomorphism

Again φ is one-one because

$$\varphi(g_1) = \varphi(g_2)$$

$$\Rightarrow f_{g_1} = f_{g_2}$$

$$f_{g_1} f_{g_2}^{-1} = f_{g_2 g_2^{-1}} = f_e$$

$$\Rightarrow g_1 g_2^{-1} = e \Rightarrow g_1 = g_2$$

or

$$f_{g_1}(x) = f_{g_2}(x) \qquad \forall x \in G$$

$$\Rightarrow g_1 x = g_2 x \qquad \forall x \in G$$

$$\Rightarrow g_1 = g_2$$

φ is onto because each $f_g \in G'$ is the image of a $g \in G$.

Thus G is isomorphic to G', a sub-group of all bijective mappings and hence G is embedded into the group of all bijective mappings.

Corollary Every finite group of order n can be embedded in a group of bijective mappings of a set of n-elements.

OR

Every finite group of order n is ~~can be~~ embedded

isomorphic to a permutation gp (transformation gp) or to a sub-group of a symmetric gp S_n.

Sh. **Proof:-** Let G be any finite gp of order n. For every $g \in G$ consider a mapping

$$f_g : G \longrightarrow G \;:\; f_g(x) = gx \quad \forall x \in G$$

Then f_g is one-one because

$$f_g(x) = f_g(y) \qquad x, y \in G$$
$$\Rightarrow gx = gy$$
$$\Rightarrow x = y$$

and f_g is onto because any element $y \in G$ is the image of $\bar{g}'y \in G$ i.e

$$f_g(\bar{g}'y) = g\bar{g}' = y$$

So f_g is a permutation on set G *

Let $G' = \{f_g : g \in G\}$ be the set of n permutation of G. Then G' is sub-gp of set(gp) of all permutations of G.

Now we show that $G \cong G'$

Let $\varphi : G \longrightarrow G'$ be defined by

$$\varphi(g) = f_g$$

We have

$$\varphi(g_1 g_2) = f_{g_1 g_2} = f_{g_1} \circ f_{g_2} = \varphi(g_1) \circ \varphi(g_2)$$

$\Rightarrow$ φ is a homomorphism.

Again φ is one-one because

$$\varphi(g_1) = \varphi(g_2)$$
$$f_{g_1} = f_{g_2}$$
$$\Rightarrow f_{g_1} \cdot f_{g_2}^{-1} = f_{g_2} \cdot f_{g_2}^{-1} = f_e$$

$\Rightarrow g_1 g_2^{-1} = e \Rightarrow g_1 = g_2$

ϕ is obviously onto because each f_g is the image of a $g \in G$.

Thus $G \cong G'$ i.e G is embedded in a gp. of bijective mappings of a set of n elements.

Remark

1): Since f_g is is a one-one mapping of a finite set G into G', it follows that f_g is also onto

2: Cayley's embedding theorem reduced the study of all finite or infinite groups to that of the groups of bijective mappings of certain sets. The structure of these subgroups gives us almost all the information that we need for a particular group.

Theorem Let R' be the group of non-zero real numbers under multiplication and Z the group of integers under addition. For each $r \in R'$ there is one and only one embedding $f_r: Z \to R'$ such that $f_r(1) = r$

Proof:- For each $r \in R'$, define a mapping $f_r : Z \to R'$ by

$$f_r(n) = r^n \quad \forall n \in Z \longrightarrow (1)$$

Then $f_r(1) = r$ and

$$f_r(m+n) = r^{m+n} = r^m \cdot r^n = f_r(m) \cdot f_r(n)$$

So f_r is homomorphism. For f_r to be an embedding we need only verify that f_r is injective. Let

$$f_r(m) = f_r(n) \quad \text{for some } m, n \in Z$$

Then $r^m = r^n$

$\Rightarrow r^{m-n} = 1 = r^0$

$\Rightarrow m-n = 0 \Rightarrow m = n$

Uniqueness:

Suppose that there is another embedding $g_r : Z \to R'$ such that

$$g_r(1) = r$$

Then

$$g_r(n) = g_r(1+1+1+1+\ldots+1) \text{ n-Times}$$
$$= g_r(1)\cdot g_r(1)\cdot g_r(1)\cdots g_r(1)$$
$$n\text{-times } (\because g_r \text{ is homomorphism})$$
$$= r^n$$
$$= f_r(n) \quad \forall n \in Z$$

Hence $g_r = f_r$

Thus embedding is unique.

Problems:

i) Find the permutation group isomorphic to the multiplicative group of the fourth roots $1, -1, i, -i$ of unity

ii) Find the permutation gp isomorphic to the group G formed by the four bilinear transformations f_1, f_2, f_3, f_4 (defined by) of the infinite Complex plane defined by

$$f_1(z) = z,\ f_2(z) = -z,\ f_3(z) = \bar{z}^{-1},\ f_4(z) = -\bar{z}^{-1}$$

iii) Find the permutation gp isomorphic to the the gp G formed by six bilinear transformations $f_1, f_2, f_3, f_4, f_5, f_6$ of the infinite complex plane defined by

$$f_1(z) = z \quad f_2(z) = \frac{1}{z}, \quad f_3 = 1 - z, \quad f_4(z) = \frac{z}{z-1}$$

$$f_5(z) = \frac{1}{1-z} \quad f_6(z) = \frac{z-1}{z}$$

Solution:-

(i) Set $G_1 = \{1, -1, i, -i\}$

Then we prove that G_1 is isomorphic to the group G' formed of the four permutations

$G_1 = \{ I, (abcd), (ac) \circ (bd), (adcb) \}$

each of degree four

we write

$A_1 = 1 \quad A_2 = i \quad A_3 = -1 \quad A_4 = -i$

$B_1 = I \quad B_2 = (abcd) \quad B_3 = (ac) \circ (bd)$

$B_4 = (adcb)$

and set up the composition tables as

	A_1	A_2	A_3	A_4
A_1	A_1	A_2	A_3	A_4
A_2	A_2	A_3	A_4	A_1
A_3	A_3	A_4	A_1	A_2
A_4	A_4	A_1	A_2	A_2

	B_1	B_2	B_3	B_4
B_1	B_1	B_2	B_3	B_4
B_2	B_2	B_3	B_4	B_1
B_3	B_3	B_4	B_1	B_2
B_4	B_4	B_1	B_2	B_3

It is obvious that if we replace

$A_1 \quad A_2 \quad A_3 \quad A_4$

by

$B_1 \quad B_2 \quad B_3 \quad B_4$

in the composition table for G_1, we replace the composition for G'

This shows that the mapping f of G_1 onto G' defined by

$f(A_1) = A_1 \quad f(A_2) = B_2, f(A_3) = B_3 \quad f(A_4) = B_4$

is an isomorphism

Note It may be verified that mapping g of G_1 onto G' defined by

$g(A_1) = B_1$. $g(A_2) = B_4$. $g(A_3) = B_3$, $g(A_4) = B_3$
is also an isomorphism.

(ii) :- The group G_1 is isomorphic to the permutation group of degree four formed by the permutations

I , (ab) , (cd) , $(ab) \circ (cd)$

we denote the four permutations by A_1, A_2, A_3, A_4 respectively

	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

	A_1	A_2	A_3	A_4
A_1	A_1	A_2	A_3	A_4
A_2	A_2	A_1	A_4	A_3
A_3	A_3	A_4	A_1	A_2
A_4	A_4	A_3	A_2	A_1

These show that if we replace
f_1, f_2, f_3, f_4
by
A_1, A_2, A_3, A_4
respectively, the composition table for G_1 becomes that for G_1'. Thus the mapping g defined by

$g(f_1) = A_1$ $g(f_2) = A_2$ $g(f_3) = A_3$ $g(f_4) = A_4$

is an isomorphic mapping of G_1 onto G_1'

(iii) The group G_1 formed by six bilinear transformation is isomorphic to the symmetric group P_3 of degree 3 formed of six permutations

I, (ab), (bc), (ca), (abc), (acb)

We denote the permutations by

A_1 A_2, A_3 A_4 A_5 A_6

and set up composition tables as

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_6	f_1	f_5	f_4	f_3
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_4	f_2	f_3	f_6	f_1
f_6	f_6	f_3	f_4	f_2	f_1	f_5

This table shows that f_1 is identity and the elements are inversible. In fact inverses of

$f_1, f_2, f_3, f_4, f_5, f_6$ are

$f_1, f_2, f_3, f_4, f_5, f_6$ respectively.

The composition is non abelian e.g

$$f_2 \circ f_3 = f_5 \neq f_6 = f_3 \circ f_2$$

If we replace $f_1, f_2, f_3, f_4, f_5, f_6$ we get the composition table for P_3 as

$\circ$	A_1	A_2	A_3	A_4	A_5	A_6
A_1	A_1	A_2	A_3	A_4	A_5	A_6
A_2	A_2	A_1	A_5	A_6	A_3	A_4
A_3	A_3	A_6	A_1	A_5	A_4	A_3
A_4	A_4	A_5	A_6	A_1	A_2	A_3
A_5	A_5	A_4	A_2	A_3	A_6	A_1
A_6	A_6	A_3	A_4	A_2	A_1	A_5

On comparing the composition tables we see that the mapping g defined by

$$g(f_1) = A_1 \quad g(f_2) = A_2 \quad g(f_3) = A_3$$
$$g(f_4) = A_4 \quad g(f_5) = A_5 \quad g(f_6) = A_6$$

is an isomorphism

Note :- 1) We may find other possible isomorphic mappings of G onto G' also. While doing this, we

may bear in mind that only elements of equal orders can be mapped on each other through an isomorphic mapping.

2): It is important to remember that if G, G' be finite groups, such that f is an isomorphic mapping of G onto G', then if we replace each element in the composition table for G by its f-image, then we obtain the corresponding composition table for G'.

The composition tables of two isomorphic groups are thus the same except for the notations for their elements.

System of Generators and Relations in a Group

Let G be a group and X be an arbitrary non-empty subset of G. The intersection K of all subgps. of G which contain the set X is a subgp of G, called the subgroup generated by X, and is denoted by

$$K = \langle X \rangle$$

(K is the gp generated by X)

Since K contains, together with every element of X, the inverse of each element of X and also, by closure law, the product of any two and therefore of finitely many elements in X and their inverses, an arbitrary element of K can be written as

$$k = x_{\alpha_1}^{\epsilon_1} \cdot x_{\alpha_2}^{\epsilon_2} \cdots x_{\alpha_m}^{\epsilon_m} \longrightarrow (1)$$

where $x_{\alpha_i} \in X$ and $\epsilon_i = \pm 1$ $i = 1, 2 \ldots m$

The expression on R.H.S of (1) is called a word in $x_{\alpha_1}, x_{\alpha_2}, x_{\alpha_3} \ldots x_{\alpha_m}$.

... set of

Generating System

A subset X of a group G is said to be a generating system of G or a system of generators for G, if the subgroup generated by X coincides with G i.e

$$G = \langle X \rangle$$

Also we say that X generates G.

Note Every arbitrary group possess at least one generating system, viz, the group itself.

Irreducible or Independent Generating System

A generating system X is said to be irreducible or independent if no proper subset of X generates the group i.e if no member of X belongs the subgroup generated by the remaining members of the same.

A group may not however, possess an idependent system of generators.

Finitely generated group G

A group G is finitely generated iff a generating set X of G is finite. Otherwise it is infinitely generated.

Theorem:- Every finite group possesses an independent generating system or little more generally every generating system of a finite group possesses an independent generating sub-system.

Proof:- Let X be any generating set of a finite gp G. Now the set M obtained on eliminating from X each such element as belongs to the subgroup generated by the remaining members of X is the required independent generating system. Clearly, we can arrive at M

after a finite number of steps.

Note:- It may be noted, however, that a finite group may possess several distinct generating systems containing different numbers of elements. As an example, consider the group G_1 formed by the six 6th roots of unity

$1, a, a^2, a^3, a^4, a^5$; $a = \cos \pi/3 + i \sin \pi/3$

The orders of the elements a, a^2, a^3, a^4, a^5 respectively are

$6, 3, 2, 3, 6$

We have

$G_1 = \langle a \rangle$, $G_1 = \langle a^5 \rangle$

Also $G_1 = \langle a^2, a^3 \rangle$

The two elements a^2, a^3 form an independent generating system inasmuch as of these two elements no one lies in the sub-group generated by the other.

An infinite group may not possess an independent generating system.

Examples of Independent Generating System

1): The set

$$\{(12), (13), \ldots\ldots (1n)\}$$

of permutations is an independent generating set for the symmetric group P_n.

We know that every member of P_n is a composite of cycles and show that every cycle is a a composite of given set

For a cycle containing the member 1, we have

$(1\, a_1\, a_2 \ldots\ldots a_k) = (1\, a_k) \circ (1\, a_{k-1}) \circ \ldots\ldots \circ (1, a_2) \circ (1\, a_1)$

For a cycle not containing the symbol 1, we have

$(b_1\, b_2 \ldots\ldots b_l) = (1\, b_1) \circ (1\, b_l) \ldots\ldots (1\, b_2) \circ (1\, b_1)$

Also since each member of the given set of

permutations contains an element not contained in any of the others, the given set is independent.

2) The set

$$\{(123), (124), \ldots\ldots (12n)\}$$

of permutations is an independent generating set for the alternating group A_n

We show that the composite of every pair of transposition is expressible as a composite of the permutations of the given set.

Each even permutation can be expressed as a composite of pairs of permutations

$(12)(13) - - - - - , (1n)$

We have

$(1\,i) \circ (12) = (12i)\ ;\ i \neq 1, i \neq 2$

$(1\,i) \circ (1j) = (1ji) = (12i) \circ (12i) \circ (12j) \circ (12i)$

$i \neq 1 \quad i \neq 2 ; j \neq , j \neq i$

3 Consider the symmetric group P_3 with elements

$I, (ab), (bc), (ca), (abc), (acb)$

Denote these elements by

$I \quad A \quad B \quad C \quad D \quad E$

respectively. Then elements $A = (ab)$ $B = (bc)$ constitute an independent generating system of P_3

The following independent relations are satisfied by A, B

$A^2 = I\ ,\ B^2 = I \quad (AB)^3 = (acb)^3 = I$

4 Show directly that the permutations

(i) $(12), (13), (14)$ generate P_4

(ii) $(123), (124)$ generate A_4

Solution (i) we have

$$(12) \circ (13) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (123) \in P_4$$

Similarly

$(12) \circ (14) = (124) \in P_4$

$(13) \circ (14) = (134) \in P_4$

and

$(12) \circ (13) \circ (14) = (123) \circ (14)$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1234) \in P_4$$

Similarly it can be proved that all other elements of P_4 are composition of the given permutations.

(ii) Similar to (i)

5 Show that the $(n-1)$ permutations

$(12), (23) \ldots\ldots (n-1, n)$

Constitute a set independent generations of P_n.

Solution we have

$(23) \circ (12) \circ (23) = (13)$,

$(34) \circ (13) \circ (34) = (14)$,

$(n-1\ n) \circ (1\ n-1) \circ (n-1, n) = (1n)$,

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$= (13)$ i.e

$(123) \circ (23)$

so that

$(12), (13) \ldots\ldots (1, n)$

belong to the group generated by the given permutations

6 Show that the two permutations

$f = (1234\ldots n), g = (12)$

Constitute a set of independent generators P_n

Solution we have

$f^{-1} \circ g \circ f = (23)$, $f^2 \circ g \circ f^2 = (34) \ldots\ldots f^{-(n-1)} \circ g \circ f^{n-1} = (n-1, n)$

7 A system consisting of the integer 1 generates the additive group I of integers. Also a system of any two mutually prime integers is an independent generating system of I

8. The system consisting of all prime integers is an independent generating system of the multiplicative group of +ve rational numbers.

Independent Relations satisfied by the members of the Independent generating System of a finite group

It is clear that the system of all possible formal products of +ve and negative powers of elements of an independent generating system X is infinite.

Since, however, G_r is finite, these products of powers cannot all be different and accordingly the members of X must necessarily be subjected to some relations of the form

$$a^{\alpha_1} b^{\beta_1} c^{\gamma_1} \cdots = a^{\alpha_2} b^{\beta_2} c^{\gamma_2} \cdots$$

or of the form

$$a^{\alpha} b^{\beta} c^{\gamma} \cdots = e$$

where a, b, c... are some different members of G_r and $\alpha, \beta, \gamma \cdots$ are some +ve or negative integers.

Of course, some of these relations must necessarily be of the form

$$a^m = e \quad b^n = e \quad \text{etc}$$

m, n etc being the orders of a, b etc respectively.

Remark It should be noted that when we say that a certain generating system is independent, it does not mean that the elements of the system are not ~~connected~~ connected by relations. In fact as shown above such relations must exist. Of course, no one element of such a system can be expressed in terms of the others.

Defining Relation & Presentation of a Group

Let X be an arbitrary set of generators for a group G.

If for $x_{\alpha_i} \in X$ and $\epsilon_i = \pm 1$, $i = 1, 2, \ldots m$ the equation

$$W(x_{\alpha_1}, x_{\alpha_2}, x_{\alpha_3}, \ldots, x_{\alpha_m}) = x_{\alpha_1}^{\epsilon_1} \cdot x_{\alpha_2}^{\epsilon_2} \cdots x_{\alpha_m}^{\epsilon_m} = e \longrightarrow (1)$$

where e is the identity of G, holds, then (1) is called a relation in G. The word W in $x_{\alpha_1}, x_{\alpha_2}, \ldots x_{\alpha_m}$ is called a relator. A group is often represented in terms of generators and relations. If a group G has a set X as a system of generators and the words $w_1, w_2, \ldots w_k$ are relators, then we write

$$G = \langle X : w_1 = w_2 = \cdots w_k = e \rangle \longrightarrow (2)$$

and read as, G is a gp generated by a set X with $w_1 = w_2 = \cdots w_k = e$ as relations

Defining Relation A collection of equations $w_1 = \cdots = w_k = e$ which hold in a gp G is called a system of defining relations if every relation in G is derivable from these. In this case (2) is called presentation of G.

A group is finitely ~~generated~~ presented if and only if it has a finite system of generators and can be defined by a finite number of defining relations.

Note Not every gp is finitely generated. For example the group of rationals under addition is not finitely generator.

Examples

1): The group C_4 of complex numbers $1, -1, i, -i$ has a presentation

$$C_4 = \langle x : x^4 = 1 \rangle$$

with x as generator and $x^4 = 1$ as a defining relation $x^4 = 1$ is also an identical relation in C_4

2: Consider the collection V_4 of real valued functions $f_1(x) = x$, $f_2(x) = -x$, $f_3(x) = 1/x$, $f_4(x) = -1/x$, under the multiplication defined by

$$g \cdot f(x) = g(f(x))$$

V_4 is a group having f_2, f_3 as generators and $f_2^2 = f_3^2 = (f_2 f_3)^2 = f_1$ as defining relations Here

$$f_2 f_3(x) = f_2(f_3(x)) = f_2(1/x) = -1/x = f_4(x)$$

put $f_1 = e$ $f_2 = a$, $f_3 = b$, then $f_4 = ab$ and presentation of V_4 is

$$V_4 = \langle a, b : a^2 = b^2 = e = (ab)^2 \rangle$$

V_4 is called Klein's 4-group.

3 A presentation for the group S_A of all bijective mappings of the set $A = \{x, y, z\}$

$$S_A = \langle \varphi, \psi : \varphi^3 = \psi^2 = (\varphi\psi)^2 = i_A \rangle$$

Here φ, ψ are given by the equations

$\varphi(x) = y$ $\varphi(y) = z$ $\varphi(z) = x$

$\psi(x) = x$ $\psi(y) = z$ $\psi(z) = y$

while i_A denotes the identity mapping of A

4 The group D_n having a presentation

$$D_n = \langle a, b : a^n = b^2 = (ab)^2 = 1 \rangle$$

is called the dihedral group of order $2n$

For $n=2$
D_2 is simply the klein's four group

5 The group Q of quaternions $\pm 1, \pm i, \pm j, \pm k$ has a presentation

$$Q = \langle a, b : a^4 = 1 \quad a^2 = b^2 = (ab)^2 \rangle$$

Here we take $a = i \quad b = j$

6 Let $\mathcal{A}$ be a class of groups defined by the law

$$x^{-1}y^{-1}xy = e \qquad \forall x, y \in A \in \mathcal{A}$$

Then $\mathcal{A}$ is called the variety of abelian gps.
If we add another law namely

$$x^m = e$$

we get the variety $\mathcal{A}_m$ of all abelian groups of exponent m
(A group G_1 is said to have exponent m iff the equation $x^m = e$ is satisfied for all $x \in G_1$ i.e $x^m = e$ is a law in G_1)

Problem: Let a group have presentation

$$G_1 = \langle a, b : \bar{a}^1 b^2 a = b^3, \; b^{-1} a^2 b = a^3 \rangle$$

Then G_1 is identity group.

Solution:

From $\bar{a}^1 b^2 a = b^3$

$$\Rightarrow (\bar{a}^1 b^2 a)^4 = b^{12}$$

$$\Rightarrow \bar{a}^1 b^8 a = b^{12} \longrightarrow (1)$$

so that $\bar{a}^2 b^8 a^2 = \bar{a}^1 b^{12} a$

$$\Rightarrow \bar{a}^2 b^8 a^2 = (\bar{a}^1 b^2 a)^6 = b^{18} \longrightarrow (2)$$

$$\bar{a}^3 b^8 a^3 = \bar{a}^1 b^{18} a = (\bar{a}^1 b^2 a)^9 = b^{27} \longrightarrow (3)$$

$b^{-1}a^2b = a^3$

Thus from equation ③ and ①, we have.

$\therefore \quad a^{-3}b^8a^3 = b^{27}$

But $a^3 = b^{-1}a^2b \qquad a^{-3} = (b^{-1}a^2b)^{-1}$

$= b^{-1}a^{-2}b$

$\therefore b^{-1}a^{-2}b\,b^8\,b^{-1}a^2b = b^{27}$

$b^{-1}a^{-2}b^8a^2b = b^{27}$

$\Rightarrow a^{-2}b^8a^2 = b^{27}$

But $a^{-2}b^8a^2 = b^{18}$

$\Rightarrow b^{18} = b^{27}$

$b^9 = 1 \longrightarrow ④$

Consequently ② becomes

$a^{-2}b^8a^2 = b^{18} = (b^9)^2 = 1$

$\Rightarrow b^8 = 1 \longrightarrow ⑤$

Hence from ④ & ⑤ we have.

$b^9 = 1$

$b^8 \cdot b = 1 \Rightarrow b = 1$

But then from

$b^{-1}a^2b = a^3$

$a^2 = a^3$

$\Rightarrow a = 1$

Hence $G = \langle 1 \rangle$ i.e. G is identity group

Cyclic Group

A Group "C" is said to be cyclic if every element of "C" is a power (multiple) of a fixed element of C.

The fixed element is called generator of 'C'

OR

A group C capable of being generated by a single element is called cyclic group.

If a cyclic group G is generated by a, then we write

$G = \{a^m : m \in I\}$ (Multiplicative form)

$G = \{na : n \in I\}$ (In additive form)

Thus a cyclic group is one all of whose elements are powers of one and the same element.

Examples

1 The additive group of integers i.e $(Z, +)$ is an infinite cyclic group.

Here 1, -1 are generators of Z

$1 \cdot 0 = 0$

$1 \cdot 1 = 1$

$2 \cdot 1 = 1+1 = 2$

$3 \cdot 1 = 3$

$4 \cdot 1 = 1+1+1+1 = 4$

$-1 \cdot (1) = -1$

$-2 \cdot 1 = -1 + -1 = -2$

$-3 \cdot 1 = -1 - 1 - 1 = -3$

Also

$1(-1) = -1$

$2 \cdot (-1) = -1 - 1 = -2$

$3(-1) = -1 - 1 - 1 = -3$

$-1(-1) = 1$

$-2(-1) = 2$

$-3(-1) = 3$

Note Each element of a cyclic group is some +ve or −ve power (multiple) of the generator.

2 $Z_4 = \{0, 1, 2, 3\}$ under add-mod 4 is cyclic group with generators 1, 3

$3+0 = 3$

$3+1 = 0 \pmod 4$

$3+2 = 1 \pmod 4$

$3+3 = 2 \pmod 4$

Now

$1+1+1+1 = 0 \pmod 4$

$1+1+1+1+1 = 5(1) = 1 \pmod 4$

Similarly $6(1) = 2 \pmod 4$

$7(1) = 3 \pmod 4$

$\Rightarrow$ 1 is a generator of Z_4

Also

$3+3+3+3 = 4(3) = 12 = 0 \pmod 4$

Similarly $5(3) = 15 = 3 \pmod 4$

$6(3) = 18 = 2 \pmod 4$

$7(3) = 21 = 1 \pmod 4$

Hence 3 is a generator of Z_4

3 $G = \{2^n : n \in Z\}$ is a cyclic group having generators 2 and $\frac{1}{2}$

$\left(\frac{1}{2}\right)^0 = 1$

$\left(\frac{1}{2}\right)^{-1} = 2$

$\left(\frac{1}{2}\right)^{-2} = 4$

$\left(\frac{1}{2}\right)^{-3} = 8$

$2^1 = 2$

$2^2 = 4$

$2^3 = 8$

4 Let $G_n = \{ e^{\frac{2\pi k i}{n}} : k = 0, 1, 2, \ldots n-1 \}$ be the group of nth roots of unity. Set $a = e^{\frac{2\pi i}{n}}$, then $a \in G_n$.

Since for any integer k, $e^{\frac{2\pi k i}{n}} = (e^{\frac{2\pi i}{n}})^k = a^k$ every element of G_n is a power of a. Hence G_n is a cyclic group generated by a

5 Let $G_7 = \{ e^{\frac{2\pi k i}{7}} : k = 0, 1, 2, \ldots 6 \}$ be the group of seventh roots of unity.

roots are

$1, w = e^{\frac{2\pi i}{7}}, w^2 = e^{\frac{4\pi i}{7}}, w^3, w^4, w^5, w^6$

$(1)^1 = 1$.

Generators of G_7 are

$w, w^2, w^3, w^4, w^5, w^6$

6 Let $G_6 = \{ e^{\frac{2\pi k i}{6}} : k = 0, 1, 2, 3, 4, 5 \}$ be sixth roots of unity.

$w = e^{\frac{2\pi i}{6}}, w^2, w^3, w^4, w^5, w^6 = 1$

Then G_6 is a cyclic group generated by $w = e^{\frac{2\pi i}{6}}$

7 The group $C_4 = \{ \pm 1, \pm i \}$ of Complex numbers is cyclic group generated by i and $-i$.

Here $i^2 = -1 \in G_4$ $\quad i^4 = 1 \in C_4$

$i^3 = -i \in G_4$ $\quad i^1 = i \in C_4$

and $(-i)^1 = -i \in C_4$

$(-i)^2 = -1 \in C_4$

$(-i)^3 = -i \in C_4$

$(-i)^4 = 1 \in C_4$

$(-i)^5 = -i \in C_4$

Theorem

(a) Every cyclic group is Abelian.
(b) The order a cyclic group is same as that of its generator.

Proof (a) Let C be a cyclic group generated by a. Then for $x, y \in C$

$$a^m = x \quad a^n = y \quad \text{for some } m, n \in Z$$

$$xy = a^m a^n = a^{m+n} = a^{n+m} = a^n \cdot a^m$$
$$= yx.$$

$\Rightarrow$ C is abelian group.
Thus every cyclic group is abelian

(b)

Let C be a cyclic group generated by a, and e the identity element in C. Let n be the order of a so that

$$a^n = e$$

Evidently, $m \in Z$ and $m < n \Rightarrow a^m \neq e$

If $m > n$ then if q is the quotient and r is the least +ve integer (remainder) when m is divided by n

$$m = nq + r \qquad 0 \leq r < n$$

So that

$$a^m = a^{nq+r} = a^{nq} \cdot a^r = (a^n)^q \cdot a^r = e \cdot a^r$$
$$\Rightarrow a^m = a^r$$

where $r = 0, 1, 2, 3, \ldots (n-1)$
$(\because 0 \leq r < n)$

By closure axiom since $a^m \in G$, therefore n distinct elements belonging to C are

$a^0, a^1, a^2, \ldots\ldots, a^{n-1}$ where $a^0 = e = a^n$

As such there are only n elements in C &

hence order of C is n which is the order of its generator.

Theorem:- (Every) A group of order n is cyclic iff it has an element of order n.

Proof:- Let G be a cyclic group of order n and let $\langle a \rangle$ be its generator.

Let $H = \{a^i \mid i \in Z\}$

Clearly H is a sub group of G.

Since G is finite, a can not be of infinite order.

$$\text{let } o(a) = m$$

We claim that H has m elements. Now $a, a^2, a^3, \ldots a^{m-1}, a^m = e$ all belong to H and no two of them are equal as $o(a) = m$.

Let $x \in H$, then $x = a^j, j \in Z$

Now $j = mk + r \quad 0 \leq r < m$, $k \& r$ are integers. Then

$$x = a^j = a^{mk+r} = (a^m)^k a^r = a^r, \text{ where}$$

$$r = 0, 1, 2, \ldots m-1$$

So any element of H is one of $a, a^2, \ldots a^{m-1}$

Hence $H = \{a, a^2, a^3, \ldots a^m\}$. This proves our claim

Since $G = \langle a \rangle$

$\therefore G \subseteq H$. In other words $G = H$ and so

$$n = o(G) = o(H) = m = o(a)$$

i.e $o(a) = n$

Conversely Let G be a group of order n and $b \in G$ be of order n. Then as before

$K = \{b^r \mid r \in Z\}$ is a sub group of G

having n elements as $o(b)=n$

Since $K \subseteq G_1$ and $o(K)=n=o(b)$, $K=G_1$

Consequently G_1 is a cyclic group generated by b

Cyclic Sub-Group

Let G_1 be any group and $a \in G_1$. Let $H=\{a^n \mid n \in Z\}$.

Let $x=a^m$ $y=a^n$ be two elements in H

Then $x\bar{y}^1 = a^n a^{-m} = a^{n-m} \in H$

$\Rightarrow$ H is subgroup of G_1.

Clearly H is a cyclic group generated by a. This sub-group is called a cyclic subgroup of G_1 generated by a and we write $H=\langle a \rangle$

Theorem: Any subgroup of a cyclic group is cyclic.

Proof: Let $G_1=\langle a \rangle$ be a cyclic group and H be a subgroup of G_1. If $H=\{e\}$, then H is Trivially cyclic. Suppose that $H \neq \{e\}$ so there exists $a^n \in H$ such that $a^n \neq e$. Then $\bar{a}^n=(a^n)^{-1} \in H$. As either n or $-n$ is a +ve integer, we can say that $a^n \in H$ for some +ve integer n.

Let k be the least +ve integer such that $a^k \in H$. If we show that $H=\langle a^k \rangle$, then it will follow that H is a cyclic group.

Let $b \in H$.

As $b \in G_1$, $b=a^m$ for some integer m.

If k does not divide m then $\exists$ integers q (quotient) and r (remainder) such that

$$m = kq + r \qquad 0 \leq r < k$$

$$\therefore a^m = a^{kq+r}$$

$$\Rightarrow a^m = (a^k)^q \cdot a^r = a^r \cdot (a^k)^q \quad \left| \because \begin{matrix} | \\ | \\ | \\ | \end{matrix} \right. \begin{matrix} kq+r \\ \\ \\ r = r+kq \end{matrix}$$

$a^m \in H$, also, since $a^k \in H$
$\therefore (a^k)^{-q} = (a^k)^{-1}(a^k)^{-1}\cdots(a^k)^{-1}$ (q times) $\in H$ by closure law

$$a^m \cdot (a^k)^{-q} = a^r$$
$$a^r = a^m (a^k)^{-q} \in H$$

But k is minimum.

$\Rightarrow r = 0$

Thus $m = kq$ and $b = (a^k)^q$

Hence $H = \langle a^k \rangle$

Corollary Any subgroup of the additive group of integers is of the form $\langle n \rangle$, where n is some non-negative integer.

Proof: Since the additive group of integers is cyclic, the result follows from the above Theorem.

Finite Cyclic Group

A cyclic group G generated by a, is finite if order of a is finite.

If G is finite cyclic group of order n, then elements of G are

$$a^0 = e, a^1, a^2, \ldots a^{n-1}, a^n = e$$

and G is presented as

$$G = \langle a : a^n = e \rangle$$

Also $a^k = e$ iff k is divisible by n.

Theorem: If G is a cyclic group generated by a such that all powers of a are not different. Then $G = \langle a \rangle$ is a finite cyclic group.

Proof: Let $n > 0$ be the order of a s.t. that

$$a^n = e$$

Given any integer s $\exists$ integers q & r s.t.

$$s = nq + r, \quad 0 \le r < n$$

$$\therefore a^s = a^{nq+r} = (a^n)^q \cdot a^r = e \cdot a^r = a^r$$

$\Rightarrow$ There are at most n distinct element
To show that no two of these n elements are equal, let us assume if possible that

$$a^x = a^y \quad , 0 < y < x < n$$

$$\Rightarrow a^{x-y} = a^y \cdot a^{-y} = a^0 = e$$

But $0 < x-y < n$ and order of a being n

$$\therefore a^{x-y} \neq e \quad i.e \quad a^x \neq a^y$$

Thus G_1 contains exactly n (finite) distinct elements.

$$a^1, a^2, \ldots\ldots, a^{n-1}, a^n$$

Hence G_1 is finite cyclic group.

Theorem:- Let G_1 be a cyclic group of finite order n and let m be +ve divisor of n. Then $\exists$ one and only one subgroup of order m. OR
To every divisor of n, there is one and and only one subgroup of G_1.

Proof: Let $G_1 = \langle a \rangle$ be a cyclic group of order n so that $a^n = e$ and $o(G_1) = o(a)$
If $m = 1$ or n, the theorem is proved.
Let $1 < m < n$. Then $m/n \Rightarrow \frac{n}{m} = q$ for some +ve integer q. Thus order of a^q is m.

Hence $H = \langle a^q \rangle$ is a cyclic subgroup of G_1 and order of H is m.

Uniqueness; Let K be another subgroup of G_1 of order m. Then K is generated by an element a^k, where k is least +ve integer such that $a^k \in K$. i.e $K = \langle a^k \rangle$

(G) And for any integer s, $a^s \in K \Rightarrow k/s$.

Now $a^n = e \in K$ ($\because K$ is sub-group)

$\Rightarrow k/n$

Thus $o(a^k) = n/k$

Hence $o(K) = o(a^k) = n/k$

But $o(K) = m$

So $n/k = m$

$n = mk$

Also $n = mq$

$\Rightarrow mk = mq$

$\Rightarrow k = q$

We get

$K = \langle a^k \rangle = \langle a^q \rangle = H$

Hence $H = \langle a^q \rangle$ is the only subgroup of G of order n.

(G) OR

$a^{km} = e = a^n$ ($\because$ order of $K = m$)

$\Rightarrow km = n$

$K = \frac{n}{m} = q$

Therefore

$a^k = a^{qr}$

Hence $K = \langle a^k \rangle = \langle a^{qr} \rangle = H$.

which proves the uniqueness.

Problem: Find all the subgroups of a cyclic group of order 12 generated by a

Solution:

The elements of cyclic of order 12 are

$a, a^2, a^3, a^4 - - - - a^{11}, a^{12} = e$

Set of +ve divisors of 12 is

$\{1, 2, 3, 4, 6, 12\}$

The subgroup corresponding to 12 is the group itself and the subgroup corresponding to 1 is $\{e\}$

The sub group of order 2 = $[a^6] = \{e, a^6\}$

The sub group of order 3 = $[a^4] = \{a^4, a^8, a^{12}=e\}$

The subgroup of order 4 = $[a^3] = \{a^3, a^6, a^9, a^{12}=e\}$

The subgroup of order 6 = $[a^2] = \{a^2, a^4, a^6, a^8, a^{10}, a^{12}=e\}$

Infinite Cyclic Group

A cyclic group $G = \langle a \rangle$ is said to be infinite if order of a is infinite.

Theorem If C is a cyclic group generated by a such that all the powers of a are distinct, then $G = \langle a \rangle$ is an infinite cyclic group.

Proof:

Let a be the generator of G. The all the powers of 'a' being different the order of a is zero (infinite)

Let us assume, if possible that G is finite and

$$a^m = a^n \quad \text{where } m > n,\ m, n \in Z$$

$$\Rightarrow a^{m-n} = a^0 = e.$$

which contradicts the assumption that a has zero (infinite) order. Hence.

$$a^m \neq a^n.$$

i.e $G = \langle a \rangle$ contains an infinite number of elements and hence G is an infinite cyclic group.

Theorem: If C is an infinite cyclic group with a, as generator, then for $m, n \in Z$

$$m \neq n \Rightarrow a^m \neq a^n$$

Proof: Suppose $m \neq n \Rightarrow a^m = a^n$

$$\Rightarrow a^{m-n} = e \longrightarrow (1)$$

Then Two possibilities arise
either a has finite order
or $m-n=0$
Since G is infinite order group, Eq ① holds only if

$$m-n=0$$
$$\Rightarrow m=n$$

which is a contradiction
$\therefore a^m \neq a^n$

Theorem: Every proper sub-group of an infinite cyclic group is itself an infinite cyclic group and as such isomorphic to the group itself.

Proof:
Let $G_1 = \langle a \rangle$ be an infinite cyclic gp. Then every member of a proper sub-group H of G_1 is some power of a
Let m be the smallest +ve integer such that $a^m \in H$
We now show that H is generated by a^m.
Let a^k be an arbitrary element of H.
There exist integers q and r such that

$$k = mq + r \qquad 0 \leq r < m$$

so that

$$a^k = a^{mq+r} = (a^m)^q \cdot a^r$$
$$a^r = a^k \cdot (a^m)^{-q}$$

Since a^k and a^{mq} are both in H
$\therefore a^r \in H$
$\therefore a^r$ But $r < m$.
a Contradiction to our assumption that m is the smallest such integer
Hence $r = 0$
$\Rightarrow k = mq$
so $a^k = (a^m)^q \Rightarrow H = \langle a^m \rangle$

i.e elements of H are

$\cdots\cdots a^{-2m}, a^{-m}, a^{0m} = e, a^{m}, a^{2m}, a^{3m}, \cdots\cdots$

Let H be finite and

$a^m = a^n$ for $m, n \in Z, m \neq n$

$\Rightarrow a^{m-n} = a^0 = e$.

But G is an infinite cyclic group

$\therefore a^m \neq a^n$ for $m \neq n$

Thus H is an infinite cyclic group.

Example. Let $C = \langle a : a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$

Then C is cyclic group of infinite order.

Solution:-

Let C is of finite order i.e $\exists$ a +ve integer n such that

$$a^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$\Rightarrow n = 0$ Hence C is of infinite order.

Generators of Cyclic Groups

A cyclic group can be generated by more than one elements e.g group Z of integers can be generated by 1 & -1. The following theorem give information about the generators of cyclic group.

Theorem:- (a) In an infinite cyclic group, there are exactly two distinct generators namely one generator and the other its inverse.

Let C be an infinite cyclic group generated by a, then the only generators of C are a & a^{-1}

(b):- Let C be a cyclic group of order n generated by 'a', then a^k for some +ve integer less than n is also a generator of C iff k and n are relatively prime i.e. $(k, n) = 1$

Proof: (a)

Let C be an infinite cyclic group generated by a i.e. $C = \langle a \rangle$. Then.

Since $a^n = (\bar{a}^1)^{-n}$

$\Rightarrow$ Every element of C, which is some power of a is also some power of $\bar{a}^1$. Therefore $\bar{a}^1$ is the other generator.

Also a & $\bar{a}^1$ are distinct i.e $a \neq \bar{a}^1$ because if

$$a = \bar{a}^1$$
$$\Rightarrow a^2 = e$$

$\Rightarrow$ C is a finite cyclic group of order 2 which contradicts the given statement that C is infinite.

Suppose that b is the third generator of C. Then

$$a = b^m \qquad b = a^\ell$$
$$\Rightarrow a = (a^\ell)^m = a^{\ell m} \longrightarrow (1)$$

But C being infinite cyclic group, $r \neq n \Rightarrow a^r \neq a^n$

(1) is satified if

$$m\ell = 1 \Rightarrow \text{either } m = 1, \ell = 1$$
$$\text{or } m = -1, \ell = -1$$

i.e either $b = a$ or $\bar{a}^1$

So there doesnot exist third generator of C other than a & $\bar{a}^1$

OR

Let $C = \langle a \rangle$ be an infinite cyclic gp. Suppose $a^n \in C$ is also a generator of C.

$\because a \in G$

$\therefore a = (a^n)^m = a^{mn}$

Since C is infinite cyclic gp, $r \neq n \Rightarrow a^r \neq a^n$.

Hence

$$mn = 1$$

$\Rightarrow$ either $m = 1, n = 1$

or $m = -1, n = -1$

i.e $a^n = a$ or $\bar{a}^1$

Thus possibly $\bar{a}^1$ is the only generator of C different from a.

Also for $a^k \in C$, $a^k = (\bar{a}^1)^{-k}$

$\Rightarrow \bar{a}^1$ is also a generator of G. Hence a and $\bar{a}^1$ are the only generators of C

OR

If a is the generator of infinite cyclic group C, then

$$(\bar{a}^1)^{-1} = a$$

so that $\bar{a}^1$ is also generator of C. However no other element of C can be generator of C because for any $a^k \in C$ if $k \neq -1$ or 1 no power of a^k is equal to a. If for some integer q

$$(a^k)^q = a$$

$$\Rightarrow a^{qk-1} = e.$$

So that a has a finite order which is a contradiction.

(b) Let $C = \langle a \rangle$ be a finite cyclic gp of order n. If $n = 1$, then $C = \langle e \rangle$ and result holds trivially. Let $n > 1$ and for some integer k $(1 \leq k < n)$ a^k be a generator of C. Then there is an integer q such that

$(a^k)^q = a$ ($\because a$ is an element of C)

$\Rightarrow a^{kq-1} = e$.

Since $a^n = e$

$\Rightarrow n \mid qk-1$

i.e there is some integer p such that

$pn = qk-1$

$qk - pn = 1$

Hence $(k, n) = 1$

Conversely suppose that $(k, n) = 1$.

Then there exist integers p & q s.t.

$pk + qn = 1$

Thus $a^{pk+qn} = a^1$

or $a = (a^k)^p \cdot (a^n)^q$.

$= (a^k)^p \cdot e = (a^k)^p$

For any integer m

$a^m = (a^k)^{pm}$

i.e every element of C is a power of a

so a^k is a generator of C

OR

For any integer k $(1 \le k < n)$ (~~let a be a generator of C~~).

Let $H = \langle a^k \rangle$

Surely

$H \subset C$

Suppose now $(k, n) = 1$. Then there exist two integers p & q such that

$kp + qn = 1$

$\Rightarrow a^{pk+qn} = a$

$\Rightarrow (a^k)^p = a$

$\Rightarrow C \subset H$.

Thus $H = G$ and a^k is a generator of C

Conversely let a^k is a generator of C so that $\exists$ an integer q, $1 \leq q \leq n$ such that

$(a^k)^q = a$

$\Rightarrow a^{kq-1} = e$

$\Rightarrow n / kq - 1$

$\Rightarrow np = kq - 1$

$kq - np = 1$

$\Rightarrow (k, n) = 1$.

Remark It follows from the above theorem that the number of generators of a cyclic group of order n is equal to the number of integers less than n and prime to n.

Problem without checking find all the generators of the cyclic group $\{a, a^2, a^3, a^4, a^5, a^6, a^7, a^8 = e\}$ of order 8

Solution: Integers less than 8 and prime to 8 are 1, 3, 5, 7. Hence a^1, a^3, a^5, a^7 are the generators of gp.

Theorem: The generators of a cyclic gp of order n are the generators a^p where p is prime to n and $0 < p < n$

Solution:

$\because a^n = e$

$\therefore (a^p)^n = (a^n)^p = e$

which shows that $o(a^p) \leq n$

Taking $q \in Z$ such that $0 < q < n$ we have pq prime to n since n is neither a factor of p, nor of q.

Let $pq = ns + r$, $0 \leq r \leq n-1$ i.e $0 \leq r < n$

Thus

$$(a^p)^q = a^{pq} = a^{ns+r} = a^{ns} \cdot a^r = (a^n)^s \cdot a^r = a^r$$

where $r = 0, 1, 2, \ldots n-1$

It is clear that $a^r \neq e$

Hence order of a^p is n and a^p is the generator of the group.

Theorem If C is cyclic group of order n generated by (a), then for any integer k, $a^k = e$ iff n/k or k is multiple of n.

Proof

Suppose $a^k = e$ with $a^n = e$.

we are to prove that n/k.

Let $n \nmid k$ and $\exists$ integers $q, r \in Z$ such that

$$k = nq + r \qquad 0 \leq r < n$$

So

$$a^k = a^{nq+r} = (a^n)^q \cdot a^r = a^r$$

$$\Rightarrow e = a^r$$

Since a has order n, so $a^r = e$ holds only if

$$r = 0$$

$$\therefore k = nq \Rightarrow n/k$$

Conversely let $n/k \Rightarrow k = nq$

$$\therefore a^k = a^{nq} = (a^n)^q = e$$

$\therefore$ k is order of a

A cyclic group ~~of prime~~ has no proper subgroup iff its order is a prime number

Theorem Every group of prime order is cyclic

Proof:- Let G be a group of order a prime p. Let $a \in G$, $a \neq e$. Then

$$H = \langle a \rangle$$

is a cyclic subgroup of G. According to Lagranges theorem order of a subgroup of a finite group divides the order of group.

Hence order of H is p or 1

Since $a \neq e$

$\therefore o(H) \neq 1$

$\Rightarrow o(H) = p$

Hence $G = H$

Thus G is a cyclic group generated by a

Theorem:- Let G be a cyclic group with at least two elements such that G has no subgroup other than $\{e\}$ and itself i.e G has no proper subgroup Then G is a cyclic group of prime order (revese is also true and is proved later)

Proof

Let $a \neq e$, $a \in G$ (this choice is possible as G has at least two elements). Then $H = \langle a \rangle$ is a subgroup of G and $a \in H \Rightarrow H \neq \{e\}$

By hypothesis $H = G$. Hence $G = \langle a \rangle$

Now we prove that G is of finite order. If not, then by theorem with statement "agp of order n is cyclic iff it has an element of order n, $o(a)$ can not be finite. Let G is not finite.

Consider $K = \langle a^2 \rangle$, K is a subgroup of G, If $K = \{e\} \Rightarrow a^2 = e \Rightarrow o(a)$ is finite, a contradiction So $K = G$ But $a \in G \Rightarrow a \in K = \langle a^2 \rangle \Rightarrow a = (a^2)^i = a^{2i}$ for some integer $i \in Z$

$\Rightarrow a^{2i-1} = e$

$\Rightarrow o(a)$ is finite, again a contradiction since G is finite

Finally suppose that G is of order n. If n is not prime, we can write $n = rs$ where $1 < r < n$. Then since r/n ~~and~~, G has a subgroup M of order r. As $1 < r < n$, $M \neq \{e\}$ and $M \neq G$. This is against the hypothesis of the theorem.

Consequently n is prime.

Problem:- Prove that $(Q, +)$ is not a cyclic gp

Solution:- Let $a \in Q$ be the generator of Q. Then by definition each element of Q must be some integral multiple of a.

But if we take $\frac{2}{3}a \in Q$

Then $\frac{2}{3}a = na$ where $n \in Z$

$\Rightarrow \frac{2}{3} = n$

which is a contradiction as $n \in Z$

$\therefore$ our supposition is wrong and so a is not the generator of Q and hence $(Q, +)$ is not cyclic

OR

If $(Q, +)$ is cyclic, there exists $q = m/n$, $m, n \in Z$, $n \neq 0$ such that $Q = gp(m/n)$. Of course $m \neq 0$. Each non-zero element of Q would then be of the form

$$\underbrace{q + q + q + q + \cdots q}_{r}$$

or of the form

$$\underbrace{-q - q - q - q - \cdots - q}_{r}$$

with some suitable choice of the +ve integer r

But $\frac{1}{2n} \in Q$

$\Rightarrow \frac{1}{2n} = \underbrace{q + \cdots + q}_{r} = rq = r\frac{m}{n}$

i.e $1-2rm=0$

But r, m are integers

$\Rightarrow 1-2rm \neq 0$

Hence a contradiction

If

$$\frac{1}{2n} = \underbrace{-q-q-q-\cdots-q}_{r}$$

$$= -\frac{rm}{n}$$

$\Rightarrow 1+2rm = 0$ which is not true as r and m are integers

Thus $(Q, +)$ is not cyclic

Problem: Every subgroup of $(Z, +)$ is a cyclic subgroup of Z

Proof: $Z = \{0, \pm 1, \pm 2, \pm 3, \cdots\}$

We know that $(Z, +)$ is an infinite cyclic group generated by -1 and $+1$.

Let H be any arbitrary subgroup of $(Z, +)$: Let m be the least +ve integer of H. we claim that m is the generator of H.

Let $x \in H$. Then either $x < 0$, $x > 0$ or $x = 0$

Case (a): If $x > 0$. Then $x > m$ and there exist integers $q_1, r_1 \in Z^+$ such that

$$x = mq_1 + r_1 \qquad 0 \leq r_1 < m$$

$\Rightarrow r_1 = x - mq_2 \in H$ ($\because H$ is subgroup)

Since m is the least +ve integer belonging to H. and $0 \leq r < m$

$\Rightarrow r_1 \notin H$ which is a contradiction

Hence $r_1 = 0$

$\therefore x = mq_1$

i.e x is multiple of m, so m generates H

Case (b). If $x < 0$. Then $x < m$ & $-x > -m$ and There are integers q_2 & r_2 such that

$m = xq_2 + r_2 \quad 0 \le r_2 < x$

$\Rightarrow r_2 = m - xq_2 \in H$

But m is least +ve integer belonging to H

$\Rightarrow r_2 = 0$

$m = xq_2$.

$-x = -mq_2 + r_2 \quad 0 \le r_2 < m$

$mq - x = r_2 \in H$

$\Rightarrow r_2 = 0$

$\Rightarrow -x = -mq_2 = m(-q_2)$

i.e x is multiple of m

Hence m generates H

Case ⊆ If $x = 0$

$x = 0 = 0 \cdot m$

x is a mulliple of m

Hence m generates H

Thus H is cyclic subgroup

Theorem Let G be a cyclic group of order a prime. Prove that G has no proper subgroups

Proof:- Let G be a cyclic group of a prime order. Then the number of subgroups of G is the same as the number of distinct divisors of p, which are p and 1. Hence the number of distinct subgroups of G is two. As $\{e\}$ & G are are two distinct subgroups, the number of proper (non-trivial subgroups is zero

OR

Let G has a sub-group $H \neq \{e\}$. Then $o(H)$ is a divisor of order of G. Since divisors of p

are 1 and p itself and $H \neq \{e\}$, $o(H) = p$.
So $H = G$
Thus G has no proper subgroup or non-Trivial subgroups.

Problem:- prove that the only groups which have no proper subgroups are the cyclic groups of order p, prime and the group consisting of the identity alone.

Solution:-

Let G be a group with no proper subgroups, $G \neq \{e\}$. Let $g \in G$, $g \neq e$. Then $K = gp(g)$ is subgroup

Since $g \in K$ and G has no proper subgp.
$\therefore K = G$

Hence $\therefore$ G is cyclic

If G is cyclic of order mn, $m, n \neq 1$, then because m divides order of G, therefore G has a subgroup of order m. But this is a proper subgroup. Hence G is cyclic of prime order or else possible infinite cyclic say $G = gp(x) = \{\ldots x^{-2}, x^{-1}, x^0, x^1, x^2 \ldots x^{-2} \ldots\}$. But $H = gp(x^2)$ is a subgroup not equal to $\{e\}$ and not equal to G since $x \notin H$. Hence G can only be cyclic of order p, a prime.

Problem If G is an abelian group, show that $(ab)^n = a^n b^n$ for all $a, b \in G$.

Solution:- Let G be an abelian gp. Then
$ab = ba \quad \forall a, b \in G$

$\Rightarrow$ statement is true for $n = 1$

let $(ab)^k = a^k b^k$, where k is +ve integer

then

$$(ab)^{k+1} = (ab)(ab)^k$$
$$= (ab)(a^k b^k)$$
$$= a(ba^k)b^k = a(a^k b)b^k \quad (\because G \text{ is abelian})$$

$= (aa^k)(bb^k) = a^{k+1}b^{k+1}$

Since the results holds for $k+1$, by mathematical induction $(ab)^n = a^n b^n$ for all +ve integer n.

Now

$(ab)^0 = e = a^0 b^0$

$\Rightarrow$ Result is true for $n = 0$

Suppose $n = -m$, where m is a +ve integer then

$(ab)^n = [(ab)^{-1}]^m = (b^{-1}a^{-1})^m$

$= (b^{-1})^m (a^{-1})^m = b^{-m} a^{-m}$

$= a^m b^{-m} = a^n b^n$

$\Rightarrow$ result is true for all -ve integer.

Hence

$(ab)^n = a^n b^n \quad \forall n \in \mathbb{Z}$

Problem:- Let G be abelian. Let $x, y \in G$ be of orders r, s respectively. Show that xy is of order rs if r and s are co-prime, i.e have no common prime divisors

Solution:- Since G is abelian

$\therefore (xy)^n = x^n y^n$ for any integer n.

Since

$(xy)^{rs} = x^{rs} y^{rs} = (x^r)^s (y^s)^r = e$

$\therefore$ order of xy divides rs

Let $o(xy) = m$. Then $m \mid rs$

Also $(xy)^m = e$.

$\Rightarrow x^m y^m = e$.

$\Rightarrow x^m = y^{-m}$

& $e = x^r = (x^r)^m = (x^m)^r = y^{-mr}$

$\Rightarrow o(y)$ divides $-mr$

i.e s divides $-mr$

Since s does not divides r $\quad \because (r,s) = 1$

$\therefore s$ must divide m

Similarly r divides m

$\Rightarrow rs / m$

Hence. $m = rs$

$o(ng) = rs$

Problem: Show that if G is a cyclic group of order $m \neq \infty$ (i.e of finite order) and s is co-prime to m, then $a^s = b^s$ $(a, b \in G)$ implies $a = b$. Find a group G and a non-zero integer n such that there are two elements $a, b \in G$ with $a^n = b^n$ but $a \neq b$

Solution: Since G is abelian

So $(ab^{-1})^s = a^s (b^{-1})^s = e$

Since $G = gp(x)$ and order of G is m, then $ab^{-1} = x^r$ for some r and

$$(ab^{-1}) = x^r$$
$$(ab^{-1})^s = x^{rs}$$
$$e = x^{rs}$$
$$\because o(G) = m$$
$$\Rightarrow m / rs$$

But m and s are co-prime.

$\therefore m / r$.

Set $r = qm$

Now. $ab^{-1} = x^r = x^{qm} = e$

$\Rightarrow a = b$

In S_3 let $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

Then $a^2 = b^2$ & $a \neq b$

Problem Show that if $G_1 = gp(x)$ and G_1 is of finite order r and s is co-prime to r, then $gp(x^s) = G_1$

Solution: The distinct elements of $G_1 = gp(x^s)$ are $e, x^s, x^{2s}, \ldots x^{(n-1)s}$, where $(x^s)^n = x^{ns} = e$ and n is the least such +ve integer.

Since $x^{ns} = e$ and $o(G_1) = r$

$\therefore \quad r \mid ns$

As r and s are co-prime

$\therefore \quad r \mid n$

Hence there are at least r distinct elements in $gp(x^s)$.

But $gp(x^s) \subseteq G_1$ and G_1 itself has only r elements

$\therefore \quad G_1 = gp(x^s)$

Theorem: (a) The number of distinct subgroups of G_1 is the same as the number of distinct divisors of $m = |G_1| < \infty$

(b) There is at most one subgroup of G_1 of any given order for G_1 finite.

Proof:

(a) Let $l_1, l_2, l_3, \ldots, l_n$ be the distinct divisors of m. Then put $H_1 = gp(x^{l_1})$, $H_2 = gp(x^{l_2})$ $\ldots\ldots$, $H_n = gp(x^{l_n})$.

Then $|H_i| = m/l_i$

These are n distinct subgroups of G_1

Now any subgroup H of G_1 will have to be generated by x^l, where l is a +ve integer dividing m. Hence $l = l_i$, for some $i = 1, 2, \ldots n$.

Therefore $H = H_i$. Thus the subgroups of G_1 are simply $H_1, H_2 \ldots\ldots, H_n$

(b) Let H and K be two subgroups of G such that

$$|H| = |K|$$

If $O(G) = n$

Then orders of H and K are $\frac{n}{l_1}, \frac{n}{l_2}$ where l_1 & l_2 are divisors of n.

Since $|H| = |K|$

$$\Rightarrow \frac{n}{l_1} = \frac{n}{l_2}$$

$$\Rightarrow l_1 = l_2$$

and $H = K$.

Remark: It can be proved that there are an infinite number of subgroups of an infinite cyclic group.

Theorem: Let Q be the group of rationals under addition. Then any two generators subgroup of Q is infinite cyclic.

Proof:- Let $H = \langle \frac{m_1}{n_1}, \frac{m_2}{n_2} \rangle$ be a two generator subgroup of Q.

If $d = (m_1, m_2)$, then there exist integers q_1, q_2 such that

$$m_1 = q_1 d \qquad m_2 = q_2 d$$

Let $a = \frac{d}{n_1 n_2}$

Since $\frac{m_1}{n_1} = q_1 \frac{d}{n_1} = q_1 n_2 \frac{d}{n_1 n_2} = q_1 n_2 a$

$$\frac{m_2}{n_2} = q_2 n_1 a$$

$\Rightarrow$ both $\frac{m_1}{n_1}$ and $\frac{m_2}{n_2}$ are in the cyclic gp generated by a. Hence

$$H \subseteq \langle a \rangle$$

As the subgroups of a cyclic group are cyclic, H is cyclic. Of Course H is infinite.

Theorem:- Let $G_1, G_2 \ldots$ be subgroups of a gp G. If $G_i \subset G_{i+1}$ $G_i \neq G_{i+1}$ for $i = 1,2,3 \ldots$ Then $\bigcup_{i=1}^{\infty} G_i$ is not a cyclic group.

Proof:- Let $K = \bigcup_{i=1}^{\infty} G_i$

First we show that K is a subgroup of G.

Let $a, b \in K$.

$\Rightarrow a \in G_m$, $b \in G_n$ for some $m, n \in Z^+$

Suppose $m < n$, then $G_m \subset G_n$

So $a, b \in G_n$

Since G_n is a subgroup of G

$\therefore ab^{-1} \in G_n$

$\Rightarrow ab^{-1} \in \bigcup_{i=1}^{\infty} G_i = K$

$\Rightarrow K$ is a subgroup of G.

Let K be cyclic and

$K = \langle a \rangle$

Then $a \in G_m$ for some integer m

As G_m is a group, every power of a belongs to G_m.

$\therefore \langle a \rangle = K = \bigcup_{i=1}^{\infty} G_i \subseteq G_m$

But $G_m \subseteq K$

Hence $G_m = K$

But then

$G_m \subset G_{m+p} \subset K = G_m \; \forall p \neq 1$

$\Rightarrow G_m = G_{m+p} \quad \forall p \neq 1$

which is a contradiction to the supposition that $G_m \neq G_{m+1}$

Hence K is not cyclic.

Theorem (a) Let φ be a homomorphism of a cyclic group G. Then
(a) $\varphi(G)$ i.e homomorphic image of a cyclic group is cyclic.

Proof: Let $G = \langle a \rangle$ and $\varphi : G \longrightarrow G'$ be a homomorphism. Then $\varphi(G)$ is homomorphic image of G.

We show that $\varphi(G)$ is cyclic

Let $\varphi(a) = b \in \varphi(G)$

Let $x \in \varphi(G)$. Then there is an element a^k in G such that

$$\varphi(a^k) = x$$

$$\varphi(a^k) = \varphi(a \cdot a \cdot a \cdot a \cdots a \text{ k times})$$

$$= \varphi(a) \cdot \varphi(a) \cdot \varphi(a) \cdots \varphi(a) \text{ k times}$$

$$x = (b)^k$$

Hence $\varphi(G)$ is a cyclic group.

OR

If $G = gp(a) = \langle a \rangle$, then

$$G = \{ a^n : n \in Z \}$$

and

$$\varphi(G) = \{ \varphi(a^n) : n \in Z \}$$

$$= \{ (\varphi(a))^n : n \in Z \} = gp(\varphi(a))$$

$\Rightarrow$ $\varphi(G)$ is cyclic group.

Theorem: (a) Every infinite cyclic group is isomorphic to the additive group of integers

(b) A finite cyclic group of order n is isomorphic to the multiplicative group of the n nth roots of unity.

Proof: (a) Let $G = \langle a \rangle$ be infinite cyclic group i.e all the powers of a are distinct.

Consider the mapping $\varphi : G \longrightarrow Z$ defined by
$$\varphi(a^k) = k \quad \text{where } k \in Z$$
Then φ is obviously surjective
Also for $a^m, a^n \in G$
$$\varphi(a^m) = \varphi(a^n)$$
$$\Rightarrow m = n$$
So φ is injective
Hence φ is bijective
$$\varphi(a^m \cdot a^n) = \varphi(a^{m+n}) = m+n$$
$$= \varphi(a^m) + \varphi(a^n)$$
$\Rightarrow \varphi$ is a homomorphism
Hence φ is an isomorphism i.e
$$G \cong Z$$
OR
Define a mapping $f : Z \longrightarrow G$ by
$$f(k) = a^k$$
Then f is obviously surjective.
Also f is one-one because
$$f(m) = f(n)$$
$$\Rightarrow a^m = a^n$$
$$\Rightarrow m = n$$
and $f(m+n) = a^{m+n} = a^m \cdot a^n = f(m) \cdot f(n)$
Hence f is an isomorphism.
Thus $Z \cong G$

(b) Let $G = \langle a \rangle$ be a finite cyclic group of order n i.e some, two different powers of a, are the same
Then elements of G are $a, a^2, \ldots, a^n = e$
Let $U_n = \left\{ e^{\frac{2k\pi i}{n}} : k = 0, 1, 2, \ldots, n-1 \right\}$ be the set of n nth roots of unity.
Define a mapping $\varphi : G \longrightarrow U_n$ by
$$\varphi(a^k) = e^{\frac{2k\pi i}{n}}$$
Then φ is obviously, surjective.

Also

$$\varphi(a^m) = \varphi(a^l)$$

$$e^{\frac{2m\pi i}{n}} = e^{\frac{2l\pi i}{n}}$$

$$\Rightarrow e^{\frac{2\pi i}{n}(m-l)} = e^0 = e$$

This holds if $m-l=0$ or $m-l$ is divisible by n. Also $m<n$, $l<n \Rightarrow m-l<n$ so n does not divide $m-l$.

$$\Rightarrow m-l=0$$

$$m = l$$

$$\therefore a^m = a^l$$

$\therefore \varphi$ is injective

Also for $a^k \& a^l \in G$

$$\varphi(a^k \cdot a^l) = \varphi(a^{k+l})$$

$$= e^{\frac{2(k+l)\pi i}{n}}$$

$$= e^{\frac{2k\pi i}{n}} \cdot e^{\frac{2l\pi i}{n}}$$

$$= \varphi(a^k) \cdot \varphi(a^l)$$

$\therefore \varphi$ is homomorphism

Hence $\varphi : G \longrightarrow U_n$ is isomorphism i.e

$$G \cong U_n$$

Theorem Any two cyclic groups of same order are isomorphic (It is also proved by alternate method)

Proof: We discuss following two cases

(i) When two groups C and C' are finite and each of order n. We show that C and C' are isomorphic to group $U_n = \left\{ e^{\frac{2k\pi i}{n}} : k = 0, 1, 2 \cdots n-1 \right\}$ of n, nth roots of unity.

Let a be generator of C, then elements of C are

$$a, a^2, \cdots\cdots a^{n-1}, e = a^n$$

Define a mapping $\varphi : C \longrightarrow U_n$ by

$$\varphi(a^k) = e^{\frac{2k\pi i}{n}}$$

Then

$$\varphi(a^k \cdot a^l) = \varphi(a^{k+l}) = e^{\frac{2(k+l)\pi i}{n}}$$

$$= e^{\frac{2k\pi i}{n}} \cdot e^{\frac{2l\pi i}{n}}$$

$$= \varphi(a^k) \cdot \varphi(a^l)$$

$\Rightarrow \varphi$ is homomorphism

φ is obviously surjective

Also if

$$\varphi(a^l) = \varphi(a^m)$$

$$\Rightarrow e^{\frac{2\pi l i}{n}} = e^{\frac{2\pi m i}{n}}$$

$$\Rightarrow e^{\frac{2\pi(l-m)i}{n}} = e^{0} = e$$

This holds if $l-m=0$ or $l-m$ divides by n

But $l-m < n$

$\therefore n \nmid l-m$

Hence $l-m=0$

$$\Rightarrow l = m$$

$$a^l = a^m$$

$\Rightarrow \varphi$ is injective.

Therefore $\varphi : C \longrightarrow U_n$ is isomorphism i.e.

$C \cong U_n$ & similarly $C' \cong U_n$

and so $C \cong C'$

(ii) Let C and C' be infinite cyclic groups. Let a be generator of C. Then every element of C is of the form $a^k : k \in Z$.

Define a mapping

$$\varphi(a^k) = k \quad \text{where } k \in Z$$

Then φ is obviously surjective.

Also for $a^k, a^p \in C$

$$\varphi(a^k) = \varphi(a^p)$$
$$\Rightarrow k = p$$
$$\Rightarrow a^k = a^p$$

so φ is injective.

Hence φ is bijective.

$$\varphi(a^k \cdot a^p) = \varphi(a^{k+p}) = k+p$$
$$= \varphi(a^k) + \varphi(a^p)$$

$\therefore \varphi$ is homomorphism

$\Rightarrow \varphi$ is an isomorphism

i.e $C \cong Z$

Similarly $C' \cong Z$,

i.e $Z \cong C'$ so $C \cong C'$

Problem Prove that if G is a finite group and H is an infinite group, then G and H are not isomorphic

Solution If $G \cong H$, there is one-one mapping from G onto H. But this is not possible since G is finite and H is infinite

Problem Prove that if G is a finite group and H is a subgroup of G, $H \neq G$, then G and H are not isomorphic

Solution: Since if two finite groups are isomorphic, they have same order. Since the order of H is less than that of G, it follows that G and H are not isomorphic

Theorem: Let H be a subgroup of G. Let $g \in G$. Prove that the set $S = \{g^{-1}hg \mid h \in H\}$ is a subgroup of G. Prove that $\psi: H \longrightarrow S$ defined by $\psi(h) = g^{-1}hg$, is an isomorphism of H onto S. If K is a finite cyclic subgroup of G which contains both H and S, prove that $H = S$

Proof: Since $H \neq \phi$, $S \neq \phi$.

Let $\bar{g}^1 h_1 g, \bar{g}^1 h_2 g \in S$. then

$$(\bar{g}^1 h_1 g)(\bar{g}^1 h_2 g)^{-1} = \bar{g}^1 h_1 g \cdot \bar{g}^1 h_2^{-1} g = \bar{g}^1 (h_1 h_2^{-1}) g \in S$$

$\because$ H is a subgroup
$\therefore h_1 h_2^{-1} \in H$

Thus S is a subgroup.

ψ is an onto mapping, since $\psi(h) = \bar{g}^1 h g$.

Also if

$$\psi(h_1) = \psi(h_2)$$
$$\Rightarrow \bar{g}^1 h_1 g = \bar{g}^1 h_2 g$$

Pre-multiplying by g and post-multiplying by $\bar{g}^1$

$$g(\bar{g}^1 h_1 g)\bar{g}^1 = g(\bar{g}^1 h_2 g)\bar{g}^1$$
$$h_1 = h_2.$$

Hence ψ is one-one and onto

Also

$$\psi(h_1)\cdot\psi(h_2) = \bar{g}^1 h_1 g \cdot \bar{g}^1 h_2 g = \bar{g}^1 h_1 h_2 g$$
$$= \psi(h_1 h_2)$$

$\Rightarrow \psi$ is a homomorphism.

Thus $H \cong S$

If K is a finite cyclic subgroup containing H and S, then H and S are both of finite order and since they are isomorphic, $|H| = |S|$. But by a previous theorem K has only one subgroup of any given order. Hence $H = S$

Theorem: Any two cyclic groups of same order are isomorphic

Proof:- Let $G_1 = \langle a \rangle$, $G_1' = \langle b \rangle$ be cyclic group, each of order m. Then

$$G_1 = \{a^0, a^1, \ldots\ldots a^{m-1}\}, \quad G_1' = \{b^0, b^1, \ldots b^{m-1}\}$$

Let $\varphi : G \longrightarrow G'$ be defined by

$$\varphi(a^i) = b^i \quad (i = 0, 1, 2, \ldots, m-1)$$

Then φ is obviously onto.

Also let

$$\varphi(a^l) = \varphi(a^m)$$

$$b^l = b^m$$

$$\Rightarrow l = m$$

Hence $a^l = a^m$

$\Rightarrow \varphi$ is one-one.

$$\varphi(a^i b^j) = \varphi(a^{i+j})$$

$$= b^{i+j} = b^i . b^j.$$

Now $0 \leq i, j \leq m-1$

$$\Rightarrow 0 \leq i+j \leq 2(m-1) = 2m-2$$

and so $i+j = \epsilon m + r$ where $0 \leq r < m-1$ and $\epsilon = 0$ or 1 Hence.

$$\varphi(a^{i+j}) = \varphi(a^{\epsilon m + r}) = \varphi(a^{\epsilon m} . a^r)$$

$$= \varphi(a^r) = b^r$$

$$\varphi(a^i)\,\varphi(a^j) = b^i b^j = b^{i+j} = b^{\epsilon m + r} = b^r$$

Hence $\varphi(a^i . a^j) = \varphi(a^i)\,\varphi(a^j)$

Thus φ is an isomorphism.

Hence $G \cong G'$

Case b when $G = \langle a \rangle$ & $G' = \langle b \rangle$ are infinite cyclic groups.

Then each element of G is uniquely of the form a^n, n an integer and G' has each element uniquely of the form b^n, n an integer.

Define a mapping

$\varphi : G \longrightarrow G'$ by

$$\varphi(a^n) = b^n$$

Then φ is one-one and onto mapping

Further

$$\varphi(a^m \cdot a^n) = \varphi(a^{m+n}) = b^{m+n}$$
$$= b^m \cdot b^n = \varphi(a^m)\,\varphi(a^n)$$

$\Rightarrow$ φ is an isomorphism and

$$G \cong G'$$

Problem: Prove that if G is cyclic of order n and p divides n, then there is a homomorphism of G onto a cyclic group of order p. What is the kernel of this homomorphism.

Solution: Let $G = gp(x)$ and $n = pm$. Let H be a cyclic group of order p, $H = gp(y)$.

Define a mapping

$$\varphi : x^i \longrightarrow y^i \quad 0 \le i \le n-1$$

φ is well defined. Elements x^i, $0 \le i \le n-1$, are all the distinct elements of G. Now let i & j be less than n, we have.

$$\varphi(x^i x^j) = \varphi(x^{i+j-\epsilon n}) \text{ where } \epsilon = 0 \text{ if } i+j \le n-1 \text{ and } \epsilon = i \text{ if } i+j \ge n$$

Then

$$\varphi(x^i \cdot x^j) = y^{i+j-\epsilon n} = y^i y^j y^{-\epsilon n}$$

Since order of y divides n

$\therefore$ $y^{-\epsilon n} = e$ $\quad -\epsilon n = -\epsilon pm$

Hence

$$\varphi(x^i \cdot x^j) = y^i y^j = \varphi(x^i)\,\varphi(y^j)$$

$\Rightarrow$ φ is a homomorphism

The kernel of φ is the set of all x^i such that $\varphi(x^i) = e$, $0 \le i \le n-1$

Since $\varphi(x^i) = y^i$

and $y^i = e$ iff p divides i

$$\text{Ker}\,\varphi = \{x^i \mid p \text{ divides } i\}$$
$$= \{x^p, x^{2p} \ldots x^{(m-1)p}\} = gp(x^p)$$

$\{\pm i, \pm 1\}$

$o(i) = 4$

If $\varphi(i^2 \cdot i^1) = \varphi(i^3)$

If $\varphi(i^2 \cdot i^3) = \varphi(i^5)$

$= \varphi(1)$

$= \varphi(i^{2+3-4})$

Hence

If $\varphi(i^k \cdot i^p) = \varphi(i^{k+p})$ if $k+p<4$

$= \varphi(i^{k+p-4})$ if $k+p$

Thus $\varphi(i^k \cdot i^p) = \varphi(i^{k+p-\epsilon 4})$

where $\epsilon = 0$ $\quad$ $k+p \le 3$

$\epsilon = 1$ if

Problem Prove that an abelian group generated by a finite number of elements of finite order is finite.

Solution: Let $G = (\{x_1, x_2, \ldots x_n\})$, $n < \infty$, and suppose G is abelian. Then every element g in G is of the form

$$g = x_{i_1}^{\epsilon_1} \cdots x_{i_r}^{\epsilon_r} \quad (x_{i_j} \in X, \epsilon_j = \pm 1) \qquad (1)$$

Since G is abelian, we can write g in the form

$$g = x_1^{\gamma_1} \cdots x_n^{\gamma_n} \quad (\gamma_1, \gamma_2, \gamma_3 \ldots \gamma_n \text{ integers}) \qquad (A)$$

To see this we need only observe that if $i_s = i_t$ for $s < t$ in (1), then

$$g = x_{i_1}^{\epsilon_1} \cdots x_{i_s}^{\epsilon_s + \epsilon_t} \cdots x_{i_r}^{\epsilon_r}$$

i.e. we can always "collect" all occurrences of any x in a product. Now if $x_1, x_2, \ldots, x_n$ are all of finite order, then the number of distinct elements given by (A) is finite. For if k_i is the order of x_i, $i = 1, 2, \ldots n$, the distinct powers of x_i are $1, x_i, x_i^2 \ldots x_i^{k-1}$. Thus the number of distinct elements given by (A) is at most $k_1 k_2 k_3 \ldots k_n$ and so G is finite.

$g = x_{i_1}^{\epsilon_1} \cdots x_{i_r}^{\epsilon_r}$

Let $g = x_1 \cdot x_{12}^{-1} \cdot x_{13}^{-1} x_{14}$

Since G is abelian, we can write as

$g = x_1 x_{13} \cdot x_{12}^{-1} x_{14}^{-1}$

$= x_1^2 \cdot x_2^{-2}$

$= x_1^{\gamma_1} \cdot x_2^{\gamma_2}$

Problem: If $g = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$

Then $g^{-1} = x_n^{-\epsilon_n} x_{n-1}^{-\epsilon_{n-1}} \cdots x_1^{-\epsilon_1} = h$.

Proof:

$$gh = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} x_n^{-\epsilon_n} \cdots x_1^{-\epsilon_1}$$

$$= x_1^{\epsilon_1} \cdots x_{n-1}^{\epsilon_{n-1}} \cdot e \cdot x_{n-1}^{-\epsilon_{n-1}} \cdots x_1^{-\epsilon_1}$$

$$= \cdots = x_1^{\epsilon_1} x_1^{-\epsilon_1} = e$$

Similarly

$$hg = e$$

Hence proved.

We have proved that if H is a subgroup of G and $x_1, x_2 \in H$, then $x_1 x_2^{-1} \in H$. We now generalize this and prove that:

Theorem If H is a subgroup of G and $X \subseteq H$, then

$$H \supseteq \{ x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} / x_i \in X, \epsilon_i = \pm 1, n \text{ a +ve integer} \}$$

Proof: We prove the theorem by induction on n.

Let $n = 1$

Then $x_1^{\epsilon_1} = x_1$ if $\epsilon_1 = 1$

$= x_1^{-1}$ if $\epsilon_1 = -1$

$\because$ H is a group and $x_1 \in H$

$\therefore$ $x_1^{-1} \in H$

$\Rightarrow x_1^{\epsilon_1} \in H$

Let $x = x_1^{\epsilon_1} \cdots x_k^{\epsilon_k} \in H$ and $x_{k+1} \in H$

Since $x, x_{k+1}^{\epsilon_{k+1}} \in H$, where $\epsilon_{k+1} = \pm 1$

$$x x_{k+1}^{\epsilon_{k+1}} = x_1^{\epsilon_1} \cdots x_{k+1}^{\epsilon_{k+1}} \in H$$

Hence $x_1^{\epsilon_1}, x_2^{\epsilon_2} \cdots x_n^{\epsilon_n} \in H$ for all n.

Now if X is "large enough" e.g. $X = H$

Then

$$H = \{ x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} / x_i \in X, \epsilon_i = \pm, n \text{ is +ve} \}$$

We ask what happens if X is not "large enough" i.e. i.e. if X is a subset of H

Theorem Let G be a group and let X be a non-empty subset of G. Let

$$S = \{ x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} / x_i \in X, \epsilon_i = \pm 1, n \text{ a +ve integer} \}$$

Then S is a subgroup of G. If H is any subgroup

Containing X, $H \supseteq S$

Proof

(i) $S \neq \phi$ because there exists $x_1 \in X$ as X is non-empty

(ii) Let $f, g \in S$

Then $f = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n}$ $(\epsilon_i = \pm 1)$

$g = y_1^{\eta_1} \cdots y_m^{\eta_m}$ $(\eta_i = \pm 1)$

where $x_i, y_i \in X$

$$g^{-1} = y_m^{-\eta_m} y_{m-1}^{-\eta_{m-1}} \cdots y_1^{-\eta_1}$$

$$fg^{-1} = x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} y_m^{-\eta_m} \cdots y_1^{-\eta_1}$$

$$= x_1^{\epsilon_1} \cdots x_n^{\epsilon_n} x_{n+1}^{\epsilon_{n+1}} \cdots x_{n+m}^{\epsilon_{n+m}}$$

where $x_{n+1} = y_m \cdots x_{n+m} = y_1$ and

$\epsilon_{n+1} = -\eta_m \cdots \epsilon_{n+m} = -\eta_1$

$\Rightarrow fg^{-1} \in S$ and S is a subgroup of G.

If $H \supseteq X$, then by previous theorem $H \supseteq S$. We denote

$S = gp(X)$ and call S the subgroup generated by X.

Note If a group can be generated by a finite set, we call it a finitely generated group.

Cosets of a Subgroup & Coset Decomposition of a Group:

Def (Right Congruence modulo a subgroup)
Let G be a group and H be a subgroup of G. Given $a, b \in G$, a is said to be right Congruent to b modulo H {symbolically $a \equiv_r b \pmod{H}$} if and only if $ab^{-1} \in H$

Theorem:- If G is a group and H is a subgroup of G. Then the relation $\equiv_r$ of right congruence modulo H is an equivalence relation. Further for any $a \in G$ the set $\{ha \mid h \in H\}$ is the equivalence class to which 'a' belongs.

Proof: Let $a, b \in G$ and e be the identity of H

(a) **Reflexivity:** Since $a\bar{a}^1 = e \in H$; $a \equiv_r a \pmod{H}$

(b) **Symmetry:** $a \equiv_r b \Rightarrow ab^{-1} \in H$

$\Rightarrow (ab^{-1})^{-1} \in H$

i.e $b\bar{a}^1 \in H$

$\Rightarrow b \equiv_r a \pmod{H}$

(c) **Transitivity:** let $a \equiv_r b \pmod{H}$, $b \equiv_r c \pmod{H}$

$\Rightarrow ab^{-1} \in H$, $b\bar{c}^1 \in H$

$\Rightarrow a\bar{c}^1 = (ab^{-1})(b\bar{c}^1) \in H$

$\Rightarrow a \equiv_r c \pmod{H}$

Thus the relation of right congruence modulo H is equivalence relation.

Let $Cl(a)$ denote the equivalence class to which a belongs i.e $Cl(a) = \{b \in G \mid b \equiv_r a \pmod{H}\}$

Let Ha denote the set $\{ha \mid h \in H\}$

Now $b \in Cl(a)$

$\Rightarrow b \equiv_r a \pmod{H}$

$\Rightarrow b\bar{a}^1 \in H \Rightarrow b = (b\bar{a}^1)a \in Ha$

Thus $Cl(a) \subseteq Ha$

Again $c \in Ha \Rightarrow c = ha$ for some $h \in H$

$\Rightarrow ca^{-1} = h \in H$

$\Rightarrow c \equiv_r a \pmod{H}$

$\Rightarrow c \in Cl(a)$

Thus $Ha \subseteq Cl(a)$

Hence $Cl(a) = Ha$

Right Coset Let G be a group and H be a subgroup of G. For any $a \in G$, the set

$$Ha = \{ha \mid h \in H\}$$

is called a right coset modulo H (or of H) determined by an element a of G.

Thus we find that the right coset Ha is nothing else but the equivalence class, determined by the relation of right congruence modulo H, to which a belongs.

Def (Left Congruence modulo a subgroup)

Let G be a group and H be a subgroup of G. Given $a, b \in G$, a is said to be left congruent to b modulo H {symbolically $a \equiv_l b \pmod{H}$} if and only if $a^{-1}b \in H$

Left Coset

Let G be a group and H be a subgroup of G. For any $a \in G$, the set

$aH = \{ah \mid h \in H\}$ is called a left coset of H determined by a

Since $eH = H = He$, Therefore H is itself a coset.

Remark: If aH and bH are such that $aH \cap bH \neq \phi$, then $aH = bH$, hence the cosets have no element in common with H i.e two cosets contain either the same elements or have

no elements in common. Also the cosets do not form a group.

Theorem: Let G be a group, H be a subgroup of G and $a, b \in G$. Then

1: H is both left and right coset.

2): $Ha = H \Leftrightarrow a \in H$ & $aH = H \Leftrightarrow a \in H$

3): $Ha = Hb \Leftrightarrow ab^{-1} \in H$

4): $aH = bH \Leftrightarrow a^{-1}b \in H$

Proof

(1) Let e be the identity of G. Then

$eH = H = He$.

$\Rightarrow H$ is both left and right coset of G

(2) Let $Ha = H$

$\Rightarrow ea \in Ha = H$ (as $e \in H$).

$\Rightarrow a \in Ha = H$.

$\Rightarrow a \in H$

Conversely let $a \in H$. Then.

$ha \in H \quad \forall h \in H$ (as H is a subgroup)

$\Rightarrow Ha \subseteq H$ ——— (1)

Also for $h \in H$, $h = (ha^{-1})a \in Ha$ ($\because ha^{-1} \in H$)

$\Rightarrow H \subseteq Ha$ ——— (2)

By (1) & (2)

$Ha = H$

(3) Let $Ha = Hb$

$\Rightarrow a \in Hb$ since $a = ea \in Ha$

$\Rightarrow a = hb$ for some $h \in H$.

$\Rightarrow ab^{-1} = h \in H$

Again Let $ab^{-1} \in H$.

$\Rightarrow ab^{-1} = h \in H$ for some $h \in H$

$\Rightarrow a = hb$

$\Rightarrow Ha = H(hb) = (Hh)b$

$= Hb$ since $Hh = H$ by (2)

Hence $Ha = Hb \Rightarrow ab^{-1} \in H$

④ Let $aH = bH$

$\Rightarrow \bar{a}^{-1}aH = \bar{a}^{-1}bH$

$\Rightarrow eH = \bar{a}^{-1}bH$

$\Rightarrow H = (\bar{a}^{-1}b)H$

$\Rightarrow \bar{a}^{-1}b \in H$ by ②

Also if $\bar{a}^{-1}b \in H$, then

$bH = e(bH) = (a\bar{a})(bH) = a(\bar{a}^{-1}b)H = aH$

Theorem Any two right (left) cosets of a subgroup H of a group G are either identical or disjoint. i.e either $aH \cap bH = \phi$ or $aH = bH$

Proof:-

Case I: If $aH \neq bH$, then we are to show that aH & bH are disjoint.

Let us assume if possible that $x \in aH \cap bH$.

$\Rightarrow x \in aH$ and $x \in bH$

$\Rightarrow x = ah_1$ and $x = bh_2$, $h_1, h_2 \in H$

$\therefore ah_1 = bh_2 \longrightarrow$ (A)

$ah_1h_2^{-1} = bh_2h_2^{-1} = be = b$

$(\bar{a}^{-1}a)(h_1h_2^{-1}) = \bar{a}^{-1}b$

$h_1h_2^{-1} = \bar{a}^{-1}b$

$\because h_1h_2^{-1} \in H$

$\therefore \bar{a}^{-1}b \in H \Rightarrow aH = bH$ which contradicts the hypothesis and hence two unequal cosets cannot have any element in common.

OR by (A)

$ah_1 = bh_2$

$ah_1h_2^{-1} = b$

$bH = (ah_1h_2^{-1})H = a(h_1h_2^{-1}H) = aH$

Case II If aH, bH are not disjoint, then we are to show that $aH = bH$

$\because aH, bH$ are not disjoint

$\therefore \exists$ an element common to aH, bH

$\Rightarrow \exists\ h_i, h_j$ such that $ah_i = bh_j$

$\Rightarrow a(h_i h_j^{-1}) = b h_j h_j^{-1}$

$\Rightarrow a = b(h_j h_i^{-1})$

$\Rightarrow ah = b(h_j h_i^{-1} h) \quad \forall h \in H.$

$\Rightarrow ah \in bH \quad \forall h \in H$

$\Rightarrow aH \subseteq bH \longrightarrow ①$

Similarly it can be proved that

$bH \subseteq aH \longrightarrow ②$

① & ② $\Rightarrow aH = bH.$

Theorem If H be a subgroup of the group G and $a \in G$ but $a \notin H$, then $\exists$ one-one mapping of H onto aH. OR The no of elements in each left coset of H is equal to the order of H.

Proof Define a mapping $\phi : H \longrightarrow aH$ by

$\phi(h) = ah \quad \forall h \in H.$

Since every element of left coset is of form ah, $h \in H$, is ϕ-image of h in H, the mapping is onto

Again let $\phi(h_1) = \phi(h_2)$

$\Rightarrow ah_1 = ah_2$

$\Rightarrow h_1 = h_2$

$\Rightarrow \phi$ is one-one

Hence ϕ is bijective and so no of elements in aH is same as those of H.

Problem If H and K are two subgroups of a group G, then for any $a, b \in G$ either $Ha \cap Hb = \phi$ or $Ha \cap Hb = (H \cap K)c$ for some c

Solution: Let $Ha \cap Hb \neq \phi$ i.e not empty.

Let $c \in Ha \cap Hb$

But $c \in Hc$, $c \in Kc$

Thus $c \in Ha \cap Hc$ and $c \in Hb \cap Kc$

$\Rightarrow Ha = Hc$, $Hb = Kc$ (Two right (left) cosets are either disjoint or identical)

$\Rightarrow Ha \cap Hb = Hc \cap Kc$

Now $H \cap K \subseteq H$

$\Rightarrow (H \cap K)c \subseteq Hc$

and $H \cap K \subseteq K \Rightarrow (H \cap K)c \subseteq Kc$.

Thus we get $(H \cap K)c \subseteq Hc \cap Kc$.

Again $d \in Hc \cap Kc \Rightarrow d = hc = kc$ $h \in H, k \in K$

$h = dc^{-1} = k \in H \cap K$

$\Rightarrow dc^{-1} \in H \cap K$

$\Rightarrow d \in (H \cap K)c$

$\Rightarrow Hc \cap Kc \subseteq (H \cap K)c$.

Hence $Ha \cap Hb = Hc \cap Kc = (H \cap K)c$.

Right and Left Coset Decomposition.

The collection of all distinct right cosets of H is called a right coset decomposition of G modulo H (or relative to H). Similarly left Coset decomposition can be defined.

Note: Define $(Ha)^{-1}$ by

$$(Ha)^{-1} = \{(ha)^{-1} : h \in H\} = \{a^{-1}h^{-1} : h \in H\}$$

Then

$$(Ha)^{-1} = a^{-1}H$$

The mapping

$$Ha \longrightarrow (Ha)^{-1} = a^{-1}H, \quad a \in G$$

which is a one-one correspondence between the collection of right and left cosets shows that the right and left cosets of H in a group G are equal in number.

Examples of Cosets

① Let $G = \{\pm I, \pm i, \pm j, \pm k\}$

and $H = \{\pm I, \pm i\}$

$jH = \{\pm j, \pm k\}$

which is the left coset of G determined by j

$kH = \{\pm j, \pm k\}$

Index of a subgroup

If H is a subgroup of G. Then the number of all distinct left (right) cosets of H in G is called the index of H in G and is denoted by $[G:H]$ or $(G:H)$

Partition of a Set

A family of subsets of a set G is a partition of G if they are disjoint and their ~~intersection~~ union is G.

Theorem: Let H be a subgroup of a group G. Then the all right (left) cosets of H in G form a partition of G:

Proof: Let $\{aH : a \in G\}$ be the collection of all left cosets of H in G. First we prove that

$$G = \bigcup_{a \in G} aH$$

$\because aH \subseteq G \quad \forall a \in G$

$\Rightarrow \bigcup_{a \in G} aH \subseteq G \longrightarrow (1)$

Again let $a \in G$.

$\because e \in H$

$\therefore a2\,ae \in aH$

$\Rightarrow a \in aH \subseteq \bigcup_{a \in G} aH$

$\Rightarrow G \subseteq \bigcup_{a \in G} aH \longrightarrow (2)$

By (1) & (2) $\quad G = \bigcup_{a \in G} aH$

Let $aH \cap bH \neq \phi$!

But $x \in aH \cap bH \Rightarrow x = ah_1 = bh_2$

$\Rightarrow a = bh_2h_1^{-1} = bh_3$

$\Rightarrow a \in bH$

$ah = bh_3h \in bH \Rightarrow aH \subseteq bH$ similarly $bH \subseteq aH$ $\Rightarrow aH = bH$

which is a contradiction because aH & bH are distinct

Lagrange's Theorem :

The order of any subgroup of a finite group divides the order of Group

OR

The Index of every subgroup of a finite gp. is a divisor of the order of the group.

Proof :- Let G be a finite group and H a subgroup of G. Let $o(G) = n$, $o(H) = m$

Let C be the collection of all left cosets of H in G. We show that C defines a partition of G.

Since C is a collection of subsets of a finite set G, C is finite.

Let r be the number of elements in C

i.e $r = (G : H)$

Then $a_1H, a_2H, \ldots\ldots\ldots a_rH$ be all left cosets of H in G

since each $a_iH \subseteq G$

$$\therefore \bigcup_{i=1}^{r} a_iH \subseteq G$$

Next let $g \in G$

$\because e \in H$

$\therefore g = ge \in gH$.

so that $g \in \bigcup_{i=1}^{r} a_iH$

Thus $G \subseteq \bigcup_{i=1}^{r} a_iH$

Therefore $G = \bigcup_{i=1}^{r} a_iH$ ⟶ (1)

Next we show that

$$a_iH \cap a_jH = \phi \quad i \neq j$$

Suppose that

$$a_iH \cap a_jH \neq \phi$$

Let $x \in a_i H \cap a_j H$

$\Rightarrow x \in a_i H$ & $x \in a_j H$

So $x = a_i h$; $x = a_j h_1$ for some $h, h_1 \in H$

Thus

$$a_i h = a_j h_1$$

$$a_i = a_j h_1 h^{-1} = a_j h_2 \in a_j H, \; h_2 = h_1 h^{-1} \in H$$

$\Rightarrow a_i \in a_j H$

Let y be any element of $a_i H$, $h' \in H$.

Then

$$y = a_i h' = a_j h_2 h' = a_j h_3 \qquad h_3 = h_2 h' \in H.$$

so that $a_i h' \in a_j H \quad \forall h' \in H$

Hence $a_i H \subseteq a_j H$

Similarly $a_j H \subseteq a_i H$

$\Rightarrow a_i H = a_j H$ a Contradiction

Hence $a_i H \cap a_j H = \phi$

Thus C defines a partition of G

Now

$$G = \bigcup_{i=1}^{r} a_i H$$

&

$$|G| = |a_1 H| + |a_2 H| + \cdots + |a_r H|$$

Define a mapping

$\varphi : H \longrightarrow aH$ by

$\varphi(h) = ah$

It is obviously onto

Also $\varphi(h_1) = \varphi(h_2)$

$a h_1 = a h_2$

$h_1 = h_2$

$\Rightarrow \varphi$ is one-one and onto

Hence $|aH| = H$

So

$$|G| = |H| + |H| + \cdots + |H| = r|H|$$

$n = mk$

So both m & k divide n.

Corollary: 1 The order of every element of a finite group is a divisor of the order of the group.

Proof:- Let G be a finite group of order n and $a \in G$ of order m. Let C be a cyclic group generated by a. Then order of C is m. Moreover, C is a subgroup of G. By Lagrange's theorem, m devides n.

Corollary: 2 Every group whose order is a prime no. is necessarily cyclic.

Proof:- Let G be a group of order p, where p is a prime number.

Let $a \in G$ and $a \neq e$. Let C be a cyclic group generated by a. The order of C is not one because $a \neq e$. Moreover, by Lagrange's theorem, the order m of C devides the order of G

Since p is a prime number and m devides p, therefore $m = p$.

Hence C as a subgroup of G, having same order as that of G, is equal to G

Since C is cyclic, G is cyclic.

Corollary: 3: A finite group of prime order has no proper subgroup.

Proof: Let G be a finite group of order p, where p is a prime. Then by Lagrange's theorem, the order of any subgroup of G is divisor of p. But p being prime has no divisor other than 1 & p and hence there is no proper subgroup of G.

Corollary: If G is of finite order n, and $g \in G$, then $g^n = e$.

Proof: Every element of G must be of finite

order. Let $g \in G$ be order m. Then m divides $|G|$ and so $|G| = qm$. Hence.

$$g^{|G|} = g^{qm} = (g^m)^q = e^q = e.$$

$$g^n = e$$

Note For a finite group G, if k is a +ve integer such that $k \mid o(G)$, it is not necessary that G contains a subgroup of order k. For example. the alternating group A_4 whose order is ~~12~~ 12 does not have any subgroup of order 6 though 6 is a divisor of order of the order of given group. However if G is Abelian (cyclic) and k is a divisor of $o(G)$, then G must contain a subgroup of order k. This will be proved later.

Problem:- If H is a subgroup of a group G and m, n are the orders of H and G respectively then prove that $a^n = e$, e being identity of G.

Solution:- Lagrange's theorem gives $n = km$, k being some eve integer

$$\therefore a^n = a^{km} = (a^m)^k = e^k = e.$$

Theorem If the order of a gp. is is a composite number, then it has proper subgroups.

Proof:- Suppose that the order n of a gp G is a composite number i.e

$$n = pq, \quad p, q \text{ integers}, \ p \neq 1, \ q \neq 1$$

Then two cases arise.

Case (a) G is cyclic with an element a, as its generator. The order of a is n. Hence $a^p \neq e$ and the cyclic group generated by a^p is a proper subgroup of G.

Case(b) G is not cyclic so that an irreducible system of generators for G contains at least

two elements. Then again, the cyclic group generated by any one of these generators is a proper subgroup of G_1.

Hence in both cases G_1 has proper subgroups.

OR

Let G_1 be a group of order n, $n = pq$, $p \neq 1, q \neq 1$ Then

(a) Either G_1 is cyclic in which case it is generated by an element a s.t

$$a^{pq} = e.$$

Thus

$$(a^p)^q = e \qquad a^p \neq 1$$ so that

$H = \langle a^p : a^{pq} = e \rangle$ is a proper subgroup of G_1.

(b) or G_1 is not cyclic, then G_1 has at least two distinct generators a & b. In this case also $H = \langle a \rangle$ is a proper subgroup of G_1.

Problem: (Poincare) If H and K are two subgroups of finite indices in G_1, then show that $H \cap K$ (are) is also of finite index in G_1.

Solution:- Let $[G_1 : H] = m$ and $[G_1 : K] = n$ and let $Ha_1, Ha_2 \text{ ------ } Ha_m$ and $Kb_1, \text{---} kb_n$ be distinct right cosets of H and K respectively.

Now we know that if H & K are two subgps. of a gp G_1 then for any $a, b \in G_1$ either $Ha \cap Kb = \phi$ or $Ha \cap Hb = (H \cap K)c$ for some $c \in G_1$.

Therefore for any $1 \leq i \leq m$ and $1 \leq j \leq n$ either $Ha_i \cap Kb_j = \phi$ or $Ha_i \cap Kb_j = (H \cap K)c_{ij}$ for some $c_{ij} \in G_1$. Also $(H \cap K)z = Hz \cap Kz$ so each right coset of $H \cap K$ is determined by intersection of right coset of H and right coset of K. Hence distinct number of right cosets of $H \cap K$ is at most equal to mn.

Theorem:- If A & B are two subgroups whose orders are relatively prime, then they intersect in the identity subgroup.

Proof Let A & B subgroups whose orders are l & m respectively and $(l, m) = 1$

If $x \in A \cap B$, then the order k of x being the divisor of the order of the cyclic subgroup of A and of B must be a factor of both l, m.

As $(l, m) = 1$

$\therefore \quad x = e$

i.e $\quad A \cap B = e$

Product of Complexes

Def. If X & Y be two complexes, then the product of X & Y is defined as

$$XY = \{ xy : x \in X, y \in Y \}$$

The complexes X & Y are said to be permutable i.e $XY = YX$ iff for any $x \in X$ and $y \in Y$, $\exists\ x' \in X$, $y' \in Y$ such that

$$xy = y'x'$$

Now since $x \in X$, $y \in Y$, $X, Y \subseteq G_1$

$\therefore xy \in G_1$ by closure property of G_1.

In general $XY \neq YX$

For example $X = \{ i, j \}$ $Y = \{ -i, k \}$

$$XY = \{ +I, -j, k, I \}$$

$$YX = \{ I, -k, j, -I \}$$

obvioviously $XY \neq YX$

As another example let

$$G_1 = \{ I, \varphi, \varphi^2, \psi, \varphi\psi, \varphi^2\psi \}$$

$$\varphi^3 = \psi^2 = (\varphi\psi)^2 = I$$

Take

$$X = [\varphi, \psi] \quad Y = [\psi, \varphi\psi]$$

Then

$$XY = [\varphi\psi, \varphi^2\psi, I, \varphi^2]$$

$$YX = \{ \psi\varphi, \psi^2, \varphi\psi\varphi, \varphi\psi^2 \}$$

$$= \{ \varphi^2\psi, I, \psi, \varphi \}$$

So

$$XY \neq YX$$

| $\varphi\psi\varphi = \psi$

| $(\varphi\psi)\cdot(\varphi\psi) = I$

| $\varphi\psi\cdot\varphi = \psi^{-1}$

| $\psi^2 = I$

| $\psi = \psi^{-1}$

| $\varphi\psi\varphi = \psi$

Remark If X and Y are subgroups of a group G_1. Then XY may or may not be a subgroup. For example

Let $X = \{ I, \psi \}$

$Y = \{I, \phi\psi\}$

be the subgps of gp $G = \{I, \phi, \phi^2, \psi, \phi\psi, \phi^2\psi\}$

Then

$$XY = \{I, (\phi)(\psi), (\psi)(\phi^2)\}$$

Since

$\phi^2 \cdot \phi^2 = \phi^4 = \phi^3 \cdot \phi = \phi$ is not in XY

So XY is not a subgroup of G.

Thus the product of two subgroups of a group G may or may not be a subgroup.

Theorem If K, L, M be three complexes in G prove that

(a) $(KL)M = K(LM)$

Hence conclude that if H is a subset of G, $a, b \in G$ then

(i) $(ab)H = a(bH)$ (ii) $H(ab) = (Ha)b$ iii) ~~$(Ha)b =$~~

(iii) $(aH)b = a(Hb)$.

(b) $K(L \cup M) = KL \cup KM$

(c) $K(L \cap M) \subseteq KL \cap KM$.

Proof:-

(a) $(KL)M = \{(xy)z : x \in K, y \in L, z \in M\}$

$= \{x(yz) : x \in K, y \in L, z \in M\}$

$= K(LM)$

OR Let $x \in K(LM)$

$\Rightarrow x = ad$ where $a \in K, d \in LM$

But $d \in LM \Rightarrow d = bc$ where $b \in L, c \in M$

Hence $x = a(bc) = (ab)c \in (KL)M$

$\Rightarrow K(LM) \subseteq (KL)M$

Similarly $(KL)M \subseteq K(LM)$

$\Rightarrow K(LM) = (KL)M$

Conclusions

(i) $(ab)H = a(bH)$

Let $K = \{a\}$, $L = \{b\}$, $M = H$

Since $(KL)M = K(LM)$

$(ab)H = a(bH)$

(ii) $H(ab) = (Ha)b$

$M(KL) = (MK)L$

$\Rightarrow H(ab) = (Ha)b$

Similarly

$(aH)b = a(Hb)$

(b) $K(L \cup M) = KL \cup KM$

$K(L \cup M) = \{xy : x \in K, y \in L \text{ or } y \in M\}$

$= \{xy : xy \in KL \text{ or } xy \in KM\}$

$= KL \cup KM$

(c) Every member of $K(L \cap M)$ is of the form xy, where $x \in K$, $y \in L \cap M$

$\therefore K(L \cap M) = \{xy : x \in K, y \in L \wedge y \in M\}$

$= \{$

Again

$x \in K, y \in L \wedge y \in M \Rightarrow xy \in KL \wedge xy \in KM$

$\Rightarrow xy \in KL \cap KM$

Thus $K(L \cap M) \subset KL \cap KM$

In general we do not have

$K(L \cap M) = KL \cap KM$.

Remark (1) A group can be expressed as a sum of complexes.

Proof If $x \in G$ & $x \notin H$, H being a subgp of G, then the complex Hx is a right coset and xH is a left coset of H in G. But cosets are not groups and they are complexes, therefore if the gp G as as a whole is is capable of forming a complex Z which consists of all the elements of the group. Then we have $Z = H + Hx + Hy + \cdots$

② The number of complexes in a group is equal to the index of a subgroup H in G and in fact it is the is the order of the group divided by the order of the subgroup H.

Inverse of a Complex

If X be a Complex of a group G, then its inverse is given by

$$X^{-1} = \{ x^{-1} : x \in X \}$$

In other words the inverse of a complex X is the set of inverses of all elements of X.

Properties of of inverse of a Complex

1) If Z_1 Z_2 are two Complexes of a group G, then $(Z_1 Z_2)^{-1} = Z_2^{-1} Z_1^{-1}$

Proof Let $x \in (Z_1 Z_2)^{-1}$

$\Rightarrow x = (z_1 z_2)^{-1}$ for $z_1 \in Z_1$, $z_2 \in Z_2$

$\Rightarrow x = z_2^{-1} z_1^{-1}$

$\Rightarrow x \in Z_2^{-1} Z_1^{-1}$ by defination

$\therefore (Z_1 Z_2)^{-1} \subseteq Z_2^{-1} Z_1^{-1}$ ⟶ (A)

Similarly if $y \in Z_2^{-1} Z_1^{-1}$.

$\Rightarrow y = z_2^{-1} z_1^{-1}$ where $z_2^{-1} \in Z_2^{-1}$, $z_1^{-1} \in Z_1^{-1}$

$= (Z_1 Z_2)^{-1}$

$\Rightarrow y \in (Z_1 Z_2)^{-1}$ by defination

$\Rightarrow Z_2^{-1} Z_1^{-1} \subseteq (Z_1 Z_2)^{-1}$ ⟶ (B)

By (A) & (B) $(Z_1 Z_2)^{-1} = Z_2^{-1} Z_1^{-1}$

2) If H is a subgroup of a group G, then $H^{-1} = H$

Proof:- $h^{-1} \in H^{-1} \Rightarrow h \in H \Rightarrow h^{-1} \in H$ ($\because$ H is subgp)

So $H^{-1} \subseteq H$

Similarly $h \in H \Rightarrow h^{-1} \in H$, H being a subgp

$\Rightarrow h = (h^{-1})^{-1} \in H$

So $H \subseteq H^{-1}$

Hence $H^{-1} = H$.

3) **Theorem** A necessary and sufficient condition for a complex H to be a subgroup is that $HH^{-1} = H$.

Proof: **Necessary Condition**

Let H be a subgroup of G.

If $ab^{-1} \in HH^{-1}$, then

$a \in H, b^{-1} \in H^{-1}$

$\Rightarrow a \in H, b \in H \Rightarrow a, b^{-1} \in H$.

$\Rightarrow ab^{-1} \in H$.

$\Rightarrow$ So $ab^{-1} \in HH^{-1} \Rightarrow ab^{-1} \in H, b \in H, b^{-1} \in H^{-1}$

i.e $HH^{-1} \subseteq H \longrightarrow (A)$

Since H is a subgp of G

$\Rightarrow e \in H$

If $h \in H \Rightarrow h = he = he^{-1} \in HH^{-1}, h \in H, e^{-1} \in H^{-1}$

$\Rightarrow H \subseteq HH^{-1} \longrightarrow (B)$

By (A) & (B)

$$H = HH^{-1}$$

Sufficient Condition:

If $HH^{-1} = H$, then we have

$HH^{-1} \subseteq H$

Let $a, b \in H$ so that $ab^{-1} \in HH^{-1}$.

$\therefore HH^{-1} \subseteq H$ and $ab^{-1} \in HH^{-1} \Rightarrow ab^{-1} \in H$

Ultimately $a \in H, b \in H \rightarrow ab^{-1} \in H$

$\Rightarrow$ H is a subgroup of G.

4) **Theorem:** Let H & K be subgroups of group G. Then HK is a subgroup of G iff $HK = KH$ i.e H & K are permutable.

Proof Let $HK = KH$

we show that HK is a subgp of G

Let x, Clearly $e \in HK$ so that $HK \neq \phi$

Let $x, y \in HK$. Then

$x = h_1 k_1$ $\quad h_1, h_2 \in H$

& $y = h_2 k_2$ $\quad k_1, k_2 \in K$

So $xy^{-1} = (h_1 k_1)(h_2 k_2)^{-1} = h_1 k_1 k_2^{-1} h_2^{-1}$

$= h_1(k_1 k_2^{-1}) h_2^{-1} = h_1 k_3 h_2^{-1}$, $k_3 = k_1 k_2^{-1} \in K$.

Now $k_3 h_2^{-1} \in KH$

Since $HK = KH$

$\therefore k_3 h_2^{-1} = h_3 k_3'$ for some $h_3 \in H$

so $xy^{-1} = h_1 h_3 k_3' = h_4 k_3'$ $k_3' \in K$

Hence $xy^{-1} \in HK$

$\therefore HK$ is a subgroup.

Q Conversely suppose that HK is a subgroup
we show that $HK = KH$.

Let $h \in H, k \in K$. Then $hk \in HK$ and

$(hk)^{-1} \in HK$ ($\because HK$ is a subgp)

but $(hk)^{-1} = k^{-1}h^{-1} \in HK$

As $(hk) = [(hk)^{-1}]^{-1}$ and $(hk)^{-1} \in HK$.

so $hk \in KH$.

Hence $HK \subseteq KH$. ⟶ (A)

Similarly let $kh \in KH$. Then

$kh = ekhe$ $\because e \in H, k \in K \Rightarrow ek \in HK$

Since both $ek, he \in HK$

$\therefore kh = ek \cdot he \in HK$ ($\because HK$ is a subgp)

so $KH \subseteq HK$ ⟶ (B)

(A) & (B) $\Rightarrow HK = KH$.

Q OR Conversely suppose that HK is a subgroup.
we show that $HK = KH$.

Let $kh \in KH$. Then

$(kh)^{-1} = h^{-1}k^{-1} \in HK$

so $[kh^{-1}]^{-1} \in kh \in HK$ ($\because HK$ is a subgp)

$\Rightarrow KH \subseteq HK$

Again $hk \in HK \Rightarrow (hk)^{-1} \in HK$

$\Rightarrow (hk)^{-1} = h_1 k_1$ for some $h_1 \in H, k_1 \in K$

$\Rightarrow hk = (h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} \in KH$

$\Rightarrow HK \subseteq KH$

Hence $HK = KH$.

2nd Method:-

Suppose that

$$HK = KH$$

we show that HK is a subgroup by showing that $(HK)^{-1} = HK$

$$(HK)^{-1} = (KH)^{-1} = K^{-1}H^{-1}$$
$$= KH \quad (\because H \& K \text{ subgps})$$
$$= HK \quad (\because H = H^{-1} \& K = K^{-1})$$

$\Rightarrow$ (HK) is a subgroup.

OR we show that HK is a subgroup by showing that $(HK)(HK)^{-1} = HK$

$$(HK)(HK)^{-1} = (HK)(K^{-1}H^{-1})$$
$$= H(KK^{-1})H^{-1}$$
$$= H(K)H^{-1} \quad (\because KK^{-1} = K)$$
$$= (HK)H^{-1}$$
$$= (KH)H^{-1} \quad (\because HK = KH)$$
$$= K(HH^{-1})$$
$$= KH \quad (\because HH^{-1} = H)$$
$$= HK \quad (\because KH = HK)$$

$\Rightarrow$ HK is a subgroup.

Now suppose that HK is a subgroup of G.

Then $(HK)^{-1} = (HK)$

$$K^{-1}H^{-1} = HK$$
$$KH = HK \quad (\because K^{-1} = K, H^{-1} = H)$$

Hence the proposition.

Corollary: 1 If H & K are subgroups of G s.t that either H or K is normal in G then HK is a subgroup of G. (A gp H is normal in G if for any $g \in G$ $Hg = gH$)

Proof Let H be a normal subgroup of G. Then for each $k \in K$, $Hk = kH \Rightarrow HK = KH$

Hence HK is a subgroup of G.

Corollary: 2 If H & K are two subgroups of an abelian gp. G. Then HK is subgroup of G

Proof In case of abelian gp, the condition $HK = KH$ is automatically satisfied so that the complex HK in this case is always a subgroup.

Note 1 It is interesting to see that if HK is a subgroup, it is essentially the same as the subgroup generated by the union of H & K i.e

$$HK = (H \cup K)$$

we have.

$$H \subseteq HK \; ; \; K \subseteq HK \; .$$

$$\Rightarrow (H \cup K) \subseteq HK \longrightarrow (A)$$

Also it is obvious that every sub-group which contains H as well as K must necessarily contain HK so that

$$(H \cup K) \supseteq HK \longrightarrow (B)$$

By (A) & (B) $\quad HK = (H \cup K)$

This result shows that in case $HK = KH$, then sub-group generated by by union of H & K i.e $(H \cup K)$ has a rather simple structure inasmuch as every element of the same can be expressed as product of an element H with an element of K

Note 2 Adopting additive notation for group composition as is customary for abelian groups, we see that if H & K are sub-groups, of an abelian gp., then the set $H+K$ consisting of the sums obtained on adding every element of H to every element of K is a sub-group.

Theorem (Product) Let H & K be two sub-groups of a group G with orders h and k respectively and let $L = H \cap K$ have order l. Then, the order of the $HK = \frac{hk}{l}$

Stated otherwise

$$o(HK) = \frac{o(H) \cdot o(K)}{o(H \cap K)}$$

Note This is analogous to the famous result in integers

viz. l.c.m of a & b $= \frac{ab}{\text{g.c.d of } a \text{ \& } b}$

Proof:- It may be noted that HK may not be a gp. we decompose K into disjoint right cosets of L

Let $K = Lk_1 \cup Lk_2 \cup \dots \cup Lk_m$

$= \bigcup_{i=1}^{m} Lk_i$ ⟶ (1)

Then $m = \frac{o(K)}{o(L)} = \frac{k}{l}$ ∵ $L \subseteq K$

$\Rightarrow k = lm$ ⟶ (2)

Further from (1)

$HK = HLk_1 \cup HLk_2 \dots \cup HLk_m$

$= H\left(\bigcup_{i=1}^{m} Lk_i\right)$

Now $L = H \cap K \subseteq H$

$\Rightarrow HL = HH = H$ (∵ H is a sub-group)

$\therefore HK = Hk_1 \cup Hk_2 \cup \dots \cup Hk_m$

$= \bigcup_{i=1}^{m} Hk_i$ ⟶ (3)

Now we claim

(i) Each Hk_i has h elements

(ii) $Hk_i \cap Hk_j = \phi$ $i \neq j$

For let $h_1 k_i = h_2 k_i$ $h_1, h_2 \in H$

$\Rightarrow h_1 = h_2$ i.e one element of H produces only one element of Hk_i

$\Rightarrow Hk_i$ has $h = o(H)$ elements

Also let $Hk_i = Hk_j$

$\Rightarrow h_1 k_i = h_2 k_j$ $i \neq j$

$\Rightarrow h_2^{-1} h_1 = k_j k_i^{-1} \in H$

But $k_j k_i^{-1} \in K$

$\therefore k_j k_i^{-1} \in H \cap K = L$

$\Rightarrow Lk_i = Lk_j$ & $i = j$

which contradicts (1) (because Lk_i are disjoint)

$o(HK) = h \cdot m = \frac{h \cdot k}{l}$ by (2)

Hence the theorem.

Conjugacy Relation & Concugacy Classes

Normal Subgroups & Conjugate Sub-groups

Transform or Conjugate of an Element

Let G be a gp. For any $a \in G$, the element gag^{-1}, $g \in G$ is called the conjugate or transform of by g.

Conjugate Elements

Let G be a gp. An element $a \in G$ is said to be conjugate to another element $b \in G$, if there exists an element $x \in G$ such that

$$a = x^{-1}bx$$

or $$b = xax^{-1}$$

Symbolically we write this relation as

$$a \sim b$$

Centralisers & Normalisers

Normaliser of a Set

Let X be an arbitrary subset of a group G. The set of all those elements of G which commute with X is called normaliser of X in G and is denoted by $N_G(X)$ or $N(X)$. Thus

$$N_G(X) = \{ a \in G : aX = Xa \}$$

Normaliser of an Element

Let a be an arbitrary element of a gp G. The set of all those elements which commute with a, is called normaliser of a and is denoted by $N_G(a)$.

Thus

$$N_G(a) = \{ x \in G : xa = ax \}$$

Remarks (1) Since $ex = xe$, at least identity element e of G is in $N_G(X)$. So $N_G(X)$ is a non empty subset of G.

(2) Since $a^k a = a a^k$ for any integer k, $N_G(a)$ contains together with a, all powers of a.

Example: Let $G = \langle a, b : a^3 = b^2 = (ab)^2 = 1 \rangle$ and $X = \{a, b\}$

The elements of G are $1, a, a^2, ab, b, a^2b$

$aX = \{a^2, ab\} \neq \{a^2, ba\} = Xa$

$a^2X = \{a^3 = 1, a^2b\} \neq \{1, ba^2\} = Xa^2$

$bX = \{ba, 1\} \neq \{ab, 1\} = Xb$

$abX = \{(ab)a, (ab)b\} = \{(ba^2)a, ab^2\}$

$= \{b, a\} \neq \{a^2b, a^2\} = Xab$

$a^2b\,X = \{a^2ba, a^2b^2\}$

$= \{ab \quad a^2\} = \{b \quad a\} = Xa^2b$

$1 (ab)^2 = 1$

$\Rightarrow ab = b^{-1}a^{-1}$

$\because b^2 = 1$

$\therefore b = b^{-1}$

$a^{-1} = a^2$

$\Rightarrow ab = ba^2$

a^2ba

$= a(ab)a$

$= a(ba^2)a$

$= aba^2$

$= ab$

So $N_G(X) = \{1\}$

Now take $Y = \{1, a, a^2\}$

Then

$1.Y = \{1, a^2, a^2\} = Y.1$

$aY = \{a, a^2, a^3\} = \{a, a^2, 1\} = \{a, a^2, 1\} = Ya$

$a^2Y = \{a^2, a^3, a^4\} = \{a^2, 1, a\} = \{a^2, 1, a\} = Y.a^2$

$= \{1.a^2, a.a^2, a^2.a^2\} = Ya^2$

$bY = \{b \quad ba \quad ba^2\}$

$Yb = \{b \quad ab \quad a^2b\}$

$= \{b \quad ba^2 \quad ba\}$

$\Rightarrow bY = Yb$

$(ab)Y = \{ab, aba, aba^2\}$

$= \{ab \quad a^3b \quad ba^3\} = \{ab, b, a^2b\}$

$= \{ab \quad b, \quad b\}$

$= \{ab \quad b\}$

$Y(ab) = \{ab \quad a^2b \quad a^3b\}$

$= \{ab, a^2b \quad b\}$

$abY = Yab$

$a^2bY = \{a^2b, a^2ba \quad a^2ba^2\}$

$= \{a^2b \quad ab \quad b\}$

$Ya^2b = \{a^2b \quad a^3b \quad a^4b\} = \{a^2b, b, ab\}$

$\Rightarrow a^2bY = Ya^2b$

Hence $N_G(X) = \{1, a, a^2, b, ab, a^2b\} = G$

$b^2 = 1 \Rightarrow b = b^{-1}$

$a^3 = 1 \Rightarrow a^{-1} = a^2$

$\boxed{ab = ba^2}$

Also

$ab.ab = 1$

$\boxed{bab = a^{-1}}$

$ba = a^{-1}b^{-1}$

$\boxed{ba = a^2b}$

aba

$= a(a^2b)$

$= b$

$(ab)a^2 = (ba^2)a^2$

$= ba = a^2b$

Example Let $G_1 = \langle a, b : a^3 = b^2 = (ab)^2 = 1 \rangle$ and $H = \{1, b\}$ be a subset (subgroup) of Group G_1. Find $N_{G_1}(H)$

Solution: Elements of G_1 are $1, a, a^2, b, ab, a^2b$

$1H = \{1, b\} = H \cdot 1$ ✓

$aH = \{a, ab\} \neq \{a \quad ba\} = Ha$

$\Rightarrow aH \neq Ha$

$a^2H = \{a^2, a^2b\} \neq \{a^2 \quad ba^2\} = Ha^2$

$\Rightarrow a^2H \neq Ha^2$

$bH = \{b, b^2\} = \{b, 1\} = \{b, b^2\} = \{b, 1\} = Hb$

$bH = Hb$ ✓

$abH = \{ab \quad ab^2\} = \{ab \quad a\}$

$Hab = \{ab \quad bab\} = \{ab \quad a^2\}$

$\Rightarrow abH \neq Hab$

$a^2bH = \{a^2b \quad a^2\}$

$Ha^2b = \{a^2b \quad ba^2b\} = \{a^2b, a\}$

ba^2b
bba
$b^2a = a$

$a^2bH \neq Ha^2b$

Hence $N_{G_1}(H) = \{1, b\} = H$

Note Let H be a subgroup of G_1.

Since $hH = Hh \quad \forall h \in H$

$\Rightarrow H \subseteq N_{G_1}(H)$

Thus the normaliser of a subgroup H of G_1 contains H

Theorem: (a) The normaliser $N_{G_1}(X)$ of a subset X of a gp G_1 is a subgroup of G_1

(b) The normaliser $N_{G_1}(a)$ of an element a, of a gp G_1 is a sub-gp of G_1.

Proof: (a) Let $N_{G_1}(X)$ be the normaliser of a subset X of a group G_1

Let $a, b \in N_G(X)$ | $\because N_G(X) \neq \phi$ because $eX = Xe$

$\Rightarrow aX = Xa$ and $bX = Xb$

Now from $bX = Xb$ we have

$b^{-1}bXb^{-1} = b^{-1}Xbb^{-1}$

$\Rightarrow Xb^{-1} = b^{-1}X$

$\therefore (ab^{-1})X = a(b^{-1}X) = a(Xb^{-1})$

$= (aX)b^{-1}$

$= (Xa)b^{-1}$

$= X(ab^{-1})$

$\Rightarrow ab^{-1} \in N_G(X)$

So $N_G(X)$ is a subgroup of G

(b) $N_G(a) \neq \phi$ because

$ea = ae \Rightarrow e \in N_G(a)$

Let $x, y \in N_G(a)$

$\Rightarrow xa = ax$ & $ya = ay$

Now $ya = ay$

$\Rightarrow ay^{-1} = y^{-1}a$

Now $(xy^{-1})a = x(y^{-1}a) = x(ay^{-1}) = (xa)y^{-1}$

$= (ax)y^{-1} = a(xy^{-1})$

$\Rightarrow xy^{-1} \in N_G(a)$

$\Rightarrow N_G(a)$ is a subgroup of G.

Note 1):- If X is a sub-group of G, then X is normal in $N_G(X)$. Furthermore, if X is a sub-group of G, X is normal in G iff $N_G(X) = G$. These facts will be proved in section 67 normal gp.

Centraliser of a Subset

Let X be an arbitrary subset of a gp. G. The set of all those elements of G which permute with every element of X is called centraliser of X in G and is denoted by $C_G(X)$. Thus

$$C_G(X) = \{ a \in G : ax = xa \quad \forall x \in X \}$$

Centraliser of an element.

Let 'a' be an arbitrary element of a gp G. The set of all those elements of G which permute with 'a', is called centralizer of 'a' in G and is denoted by $C_G(a)$. Thus

$$C_G(a) = \{ x \in G : ax = xa \}$$

Remark 1) Centraliser and normaliser of an element of 'a' gp G are identical. However generally, the centraliser of X is different from its normaliser.

2) The centraliser of an element, of course, contains that element. In fact the centraliser of an element 'a' contains the cyclic sub-gp generated by a. However the centralizer of a subgroup need not contain that group.

Example Let $Q = \{ \pm I, \pm i, \pm j \pm k \}$

and $X = \{ i, j \}$ find $C_Q(X)$

$(\pm I)i = \pm i = i(\pm I)$

$(\pm I)j = \pm j = j(\pm I)$

But no other element of Q commute with elements of X.

Thus $C_Q(X) = \{ \pm I \}$

Similarly if $X = \{\pm I, \pm i\}$, then
$C_Q(X) = \{I, -I, i, -i\}$

Exercise Let $G_1 = \langle a, b, a^3 = b^2 = (ab)^2 = 1 \rangle$
Find the centralisers of
$H_1 = \{1\}$, $H_2 = \{1, a, a^2\}$, $H_3 = G_1$

(a) $H_1 = \{1\}$
Elements of G_1 are $1, a, a^2, b, ab, a^2b$

$1 \cdot a = a = a \cdot 1$ $\quad$ $ab \cdot 1 = ab = ab \cdot 1$
$1 \cdot a^2 = a^2 = a^2 \cdot 1$ $\quad$ $a^2b \cdot 1 = a^2b = a^2b \cdot 1$
$1 \cdot b = b = b \cdot 1$

Since all elements of G_1 commute with element of H_1
$\therefore$ $C_{G_1}(H_1) = G_1$

(b) $H_2 = \{1, a, a^2\}$
1 commutes with elements of H_2

$a \cdot 1 = 1 \cdot a$
$a \cdot a = a^2 = a \cdot a$
$a \cdot a^2 = 1 = a^2 \cdot a$
} $\Rightarrow$ a commutes with all elements of H_2.

$a^2 \cdot 1 = 1 \cdot a^2 = a^2$
$a^2 \cdot a = a^3 = 1 = a \cdot a^2$
$a^2 \cdot a^2 = a = a^2 \cdot a^2$
} $\Rightarrow$ a^2 commutes with all elements of H_2

$b \cdot 1 = 1 \cdot b = b$
$ba \neq ab$
} $\Rightarrow$ b does not commutes with all elements of H_2

$ab \cdot 1 = ab = 1 \cdot ab$
$a \cdot ab = a^2b \neq aba = a^3b = b$
} ab does not commutes with all elements of H_2
$1 \cdot a^2b = a^2b = a^2b \cdot 1$
$a \cdot a^2b = a^3b = b \neq a^2b \cdot a = a^2 \cdot a^2b = ab$

$\Rightarrow$ a^2b does not commute with all elements of H_2

So $C_G(H_2) = \{1, a, a^2\}$

($\subseteq$) $H_3 = \{1, a, a^2, b, ab, a^2b\}$

only 1 commute with all elements of H_3

So $C_G(H_3) = \{1\}$

Example Let

$G = \langle a, b, c : a^3 = b^2 = (ab)^2 = c^2 = (bc)^2 = 1, ac = ca \rangle$

Find the centraliser of the subgroup

$H = \langle a, b : a^3 = b^2 = (ab)^2 = 1 \rangle$

Solution Elements of G are

$1, a, a^2, b, ab, a^2b, c, ac, a^2c, bc, abc, a^2bc$

and

$H = \{1, a, a^2, b, ab, a^2b\}$

$1 \cdot 1 = 1 \cdot 1$ $\quad$ $1 \cdot (ab) = ab = (ab) \cdot 1$

$1 \cdot a = a = a \cdot 1$ $\quad$ $1 \cdot (a^2b) = a^2b = (a^2b) \cdot 1$

$1 \cdot a^2 = a^2 = a^2 \cdot 1$

$1 \cdot b = b = b \cdot 1$

$\Rightarrow$ 1 permutes with every element of H.

$1 \cdot a = a = a \cdot 1$ $\quad$ $ab \neq ba$

$a \cdot a = a^2 = a \cdot a$

$a^2 \cdot a = a^3 = a \cdot a^2$

$\Rightarrow$ a does not permute with every element of H

$a^2 \cdot 1 = a^2 = 1 \cdot a^2$ $\quad$ $a^2b \neq ba^2$

$a \cdot a^2 = a^3 = a^2 \cdot a$

$a^2 \cdot a^2 = a^4 = a^2 \cdot a^2$

$\Rightarrow$ a^2 doesnot permute with every element of H.

b: Since $ab \neq ba$

$\Rightarrow$ b does not permute with every element of H

Since $a \cdot (ab) = a^2b$

$(ab)a = (ba^2)a = b \Rightarrow a(ab) \neq (ab)a$

$\Rightarrow$ ab does not permute with every element of H.

Since $a\cdot(a^2b) = a^3b = b$

$(a^2b)\cdot a = a^2(ba) = a^2ba = ab$

$\Rightarrow$ $a\cdot(a^2b) \neq (a^2b)\cdot a$

$\Rightarrow$ a^2b does not permute with every element of H

$1\cdot c = c = c\cdot 1$

$ac = ca$ (given)

$a^2\cdot c = a(ac) = aca$

$c\cdot a^2 = (ca)a = aca$

$\Rightarrow a^2\cdot c = c\cdot a^2$

$b\cdot c = cb$

$b\cdot ab = acb$

$ab\cdot c = acb$

$\Rightarrow c\cdot ab = ab\cdot c$

$c\cdot a^2b = caba = bca$

$a^2b\cdot c = bac = bca$

$(bc)^2 = 1$

$bc = c^{-1}b^{-1}$

$\because b^2 = 1$

$\Rightarrow b = b^{-1}$

$\because c^2 = 1$

$c = c^{-1}$

$\Rightarrow bc = cb$

$\Rightarrow$ c permutes with every element of H.

Since $b\cdot ac = a^2bc$

$ac\cdot b = abc$

$\Rightarrow$ bc does not permute with every element of H

Since $b\cdot a^2c = ba\cdot ac = baca$

$a^2c\cdot b = a^2bc = bac$

$\Rightarrow b\cdot a^2c \neq a^2c\cdot b$

$\Rightarrow$ a^2c does not permute with every element of H

Since $(ab)\cdot(bc) = ab^2c = ac$

$(bc)\cdot(ab) = cb\cdot ba^2 = ca$

$\Rightarrow$ bc does not permute with every element of H

Since $a\cdot(abc) = a^2bc = bac$

$(abc)\cdot a = abac = ba^2ac = bc$

$\Rightarrow$ abc does not permute with every element of H.

Since $a\cdot(a^2bc) = a^3bc = bc$

$(a^2bc)\cdot a = (a^2b)(ca) = a^2bac = a^2\cdot a^2bc$

$= abc$

$\Rightarrow$ a^2bc does not permute with every element of H

Hence $C_G(H) = \{1, c\} = \langle c : c^2 = 1 \rangle$

obviously $C_G(H)$ does not contain H

Theorem: (a) Centraliser of a subset X of a gp G in G is a subgroup.

(b) centraliser of an element of gp G in G is gp.

Proof: (a) Let $a, b \in C_G(X)$. Then

$ax = xa$ & $bx = xb$ $\forall x \in X$

Now $bx = xb$

$\Rightarrow b^{-1}x = xb^{-1}$

Thus $(ab^{-1})x = a(b^{-1}x) = a(xb^{-1})$

$= (ax)b^{-1}$

$= (xa)b^{-1} = x(ab^{-1})$ $\forall x \in X$

Hence $C_G(X)$ is a subgp. of G.

(b) Let $x, y \in C_G(a)$

Then $xa = ax$ & $ya = ay$

Now $ya = ay$.

$\Rightarrow ay^{-1} = y^{-1}a$

Thus $(xy^{-1})a = x(y^{-1}a) = x(ay^{-1})$

$= (xa)y^{-1} = (ax)y^{-1}$

$= a(xy^{-1})$

$\Rightarrow xy^{-1} \in C_G(a)$

Hence $C_G(a)$ is a subgroup.

Remark If X is an abelian sub-gp of G, then X is normal in $C(X)$. This fact will be proved in normal gps.

Centre of a Group

Let G be a group. Then the set of those elements of G, which commute with every element of G is called centre of G. It is denoted by $Z(G)$ or $Z(G)$.

Thus $Z(G) = \{z \in G : zx = xz \quad \forall x \in G\}$

So centre of gp G is the centraliser of whole gp G in G i.e $C_G(G)$

If $Z(G) = \{e\}$, then G is called a gp without centre or with trival centre.

Note
- Centre of a gp G is the abelian part of G
- The centre of a gp G coincides with G iff G is abelian.

Examples

1) In the gp Q of quaternions $\pm 1, \pm i, \pm j, \pm k$, the quaternions ± 1 form the centre Q
2) The gp $S = \langle a, b : a^3 = b^2 = (ab)^2 = 1 \rangle$ has trivial centre.
3) The centres of groups Z, Q, R, and C of integers rationals, reals and of complex numbers are the corresponding groups themselves.

Theorem The centre of G is a sub-gp of G

Proof:- Since $Z(G) = C_G(G)$ and $C(G)$ is a sub-group of G, $Z(G)$ is a sub-gp of G.

OR

Let $Z(G)$ be the centre of G and $x, y \in Z(G)$ Then

$$ax = xa \quad \& \quad ay = ya \quad \forall a \in G$$

Now $ay = ya$

$\Rightarrow y^{-1}a = a y^{-1} \quad \forall a \in G$

$$(xy^{-1})a = x(y^{-1}a) = x(ay^{-1})$$

$= (xa)\bar{y}^1 = (ax)\bar{y}^1 = a(x\bar{y}^1) \quad \forall a \in G_1$

$\Rightarrow x\bar{y}^1 \in \zeta(G_1)$

$\Rightarrow \zeta(G_1)$ is a sub-group.

OR

$ax = xa = x(\bar{y}^1 y)a \quad (\because \bar{y}^1 y = e$

$= (x\bar{y}^1)(ya)$

$\therefore ax = (x\bar{y}^1)(ya) = (x\bar{y}^1)(ay)$

$\Rightarrow (ax)\bar{y}^1 = (x\bar{y}^1)a$

$\Rightarrow a(x\bar{y}^1) = (x\bar{y}^1)a$

$\Rightarrow x\bar{y}^1 \in \zeta(G_1)$

Hence $\zeta(G_1)$ is a sub-gp of G_1.

Remark

- The centre of gp G_1 is abelian sub-gp
- The centre of gp G_1 is normal sub-gp which will be proved later on.
- An element a is in the centre of G_1 iff. $N_{G_1}(a) = G_1$

Problem Show that $\zeta(G_1) = \cap\{C_{G_1}(x) / x \in G_1\}$ where $C_{G_1}(x) = \{y \in G_1 / yx = xy\}$

Solution

Let $a \in \zeta(G_1)$

$\Rightarrow ag = ga \quad \forall g \in G_1$

$\Rightarrow a \in C_{G_1}(x) \quad \forall x \in G_1$

$\Rightarrow a \in \cap\{C_{G_1}(x) / x \in G_1\}$

$\Rightarrow \zeta(G_1) \subseteq \cap\{C_{G_1}(x) / x \in G_1\} \longrightarrow (A)$

Again let $b \in \cap\{C_{G_1}(x) / x \in G_1\}$

$\Rightarrow b \in C_{G_1}(x) \quad \forall x \in G_1$

$\Rightarrow bx = xb \quad \forall x \in G_1$

$\Rightarrow b \in \zeta(G_1)$

$\Rightarrow \cap\{C_{G_1}(x) / x \in G_1\} \subseteq \zeta(G_1) \longrightarrow (B)$

$\Rightarrow$

Conjugacy Relation

By Ⓐ & Ⓑ

$$Z(G) = \bigcap \{ C_G(x) \mid x \in G \}$$

i.e Centre a gp is equal to intersection of centralisers of all elements of G.

Problem: Prove that

$$C_G(x) \subseteq C_G(y) \text{ iff } y \in Z[C_G(x)]$$

Solution Let $C_G(x) \subseteq C_G(y)$

$\Rightarrow$ Every element of $C_G(x)$ is $C_G(y)$

$\Rightarrow$ Every elements of $C_G(x)$ permute with y

$\Rightarrow$ $y \in Z(C_G(x))$

Conversely let $y \in Z(C_G(x))$

$\Rightarrow$ y permutes with every element of $C_G(x)$

$\Rightarrow$ Now let g be any element of $C_G(x)$

Then

$$gx = gxg \Rightarrow x = g^{-1}xg$$

and

$$yx = yg^{-1}xg = yg^{-1}gx = yx$$

$\Rightarrow$ y permutes with x

$\Rightarrow$ $y \in C_G(x)$

$\Rightarrow$ Every element of $C_G(x)$ permutes with y

$\Rightarrow$ $C_G(x) \subseteq C_G(y)$

Conjugacy Relation & Conjugacy Classes
Normal & Conjugate Subgroups

Transform or Conjugate of an element

Let G be a group. For any $a \in G$, the element gag^{-1}, $g \in G$ is called the conjugate or transform of a, by g.

Conjugate Elements

Let G be a gp. An element $a \in G$ is said to be conjugate to another element $b \in G$, if there exists an element $x \in G$ such that

$$b = xax^{-1}$$
$$\text{or } a = x^{-1}bx.$$

Symbolically this relation is written as $a \sim b$

Two elements $a, b \in G$ are said to be conjugate iff $\exists$ an element $g \in G$ s.t. that $b = gag^{-1}$

Example Let $G = \langle a, b,\ a^3 = b^2 = (ab)^2 = 1 \rangle$
what is the conjugate of b & a

Solution: Elements of G are $1, a, a^2, b, ab, a^2b$

Conjugates of b

$1\,b\,1^{-1} = b$

$a\,b\,a^{-1} = aba^2 = a^2b$

$a^2\,b\,(a^2)^{-1} = a^2ba^{-2} = a^2ba = ba^2 = ab$

$b\,b\,b^{-1} = b^2b^{-1} = b^{-1} = b$

$(ab)\,b\,(ab)^{-1} = (ab)\,b\,(ab) = ab^2ab = a^2b$

$(a^2b)\,b\,(a^2b)^{-1} = (a^2b)b(b^{-1}a^{-2}) = (a^2b)b(ba) = a^2b\,b^2a = a^2ba = ab$

Thus conjugates of b are b, a^2b, ab

Conjugate of a

$1\,a\,1^{-1} = a$

$a\,a\,a^{-1} = a^2a^2 = a$

$a^2\,a\,a^{-2} = a^2a \cdot a = a$

$bab^{-1} = bab = a^2b \cdot b = a^2$

$(ab)\,a\,(ab)^{-1} = (ab)\,a\,(ab) = (ab)(a^2b) = (ab)(ba) = ab^2a = a^2$

$(a^2b)\,a\,(a^2b)^{-1} = (a^2b)\,a\,(b^{-1}a^{-2}) = (a^2b)\,a\,(ba) = a^2b^2a = a^2$

⇒ Conjugates of a are a, a^2

This also shows that b is not conjugate to a

Example Let G be an abelian gp. Then an element a of G can be conjugate to only itself

Theorem: Let G be a gp. Then the relation of conjugacy between elements of G is an equivalence relation.

Proof: 1) Reflexivity

Let $a \in G$.

Since $a = eae^{-1}$

$\therefore a \sim a$ i.e relation of conjugacy is reflexive

2) Symmetry:

Let $a \sim b$, $a, b \in G$

$\Rightarrow$ ∃ an $x \in G$ such that

$b = xax^{-1}$

so $a = x^{-1} b (x^{-1})^{-1}$

$\Rightarrow b \sim a$

3) Transitivity

Let $a \sim b$, $b \sim c$

$\Rightarrow$ ∃ two elements x, y of G such that

$b = xax^{-1}$ $c = yby^{-1}$

$\Rightarrow c = yxax^{-1}y^{-1} = (yx)a(yx)^{-1}$

$\Rightarrow a \sim c$

⇒ Relation of Conjugacy is transitive and hence is an equivalence relation.

Equivalence Classes of Conjugate Elements

Since the relation of conjugacy between the elements of a gp G is equivalence relation, it partitions G into mutually disjoint equivalence classes known as classes of conjugate elements or classes of gp. such that

(i) any two members of the same class are conjugate

(ii) no two members of different classes are conjugate.

Conjugacy Class

Let G_1 be a gp and $a \in G_1$. Then set of all those elements of G which are conjugate to a is called conjugacy class determined by an element $a \in G_1$ and is denoted by C_a, C_a or $\bar{a}$. Thus

$$C_a = \{ b \in G_1 : b = xax^{-1} \text{ for some } x \in G_1 \}$$

OR

Let G_1 be a group and $a \in G_1$. Then the set $C_a = \{ b \in G_1 : xax^{-1} = b \text{ for some } x \in G_1 \}$ is called the conjugacy class determined by an element $a \in G_1$

Example Let $G_1 = \langle a, b : a^3 = b^2 = (ab)^2 = 1 \rangle$

Then

$$C_b = \bar{b} = \{ b, ab, a^2b \} = C_{ab}$$

$$C_a = \{ a, a^2 \} = C_{a^2}$$

$$C_1 = \{1\}$$

Example Let $G_1 = \langle a ; a^4 = 1 \rangle$ be a cyclic gp. of order 4 under multiplication. Find conjugacy classes in G_1

Solution $G_1 = \{1, a, a^2, a^3\}$

$$C_1 = \{1\}$$

$$C_a = \{a\}$$

$$C_{a^2} = \{a^2\}$$

$$C_{a^3} = \{a^3\}$$

Note • In an abelian gp, no two elements are conjugate. Hence in this case there are as many conjugacy classes as the number of elements in that gp. i.e In an abelian group, every elmt is conjugate to only itself

• Since every cyclic gp is abelian, above fact is true for cyclic gp also. as is clear from example.

Class Equation of a Group

Let G be a finite gp of order n. Then the number of conjugacy classes in G is also finite.

Let $Ca_1, Ca_2, \ldots\ldots Ca_r$ be all conjugacy classes in G; let m_i be the no of elements in $Ca_i, i=1,2\ldots r$

Since these conjugacy classes are pairwise disjoint and their union is G, we get

$$o(G) = |G| = n = m_1 + m_2 + m_3 + \ldots + m_r$$

$$|G| = \sum_{i=1}^{r} m_i = \sum_{i=1}^{r} |Ca_i|$$

This equation is called the class-equation of G. Sum of the orders of all conjugacy classes of G is equal to the order of G

Properties of Conjugacy Classes

(i) Every element appears in one and only one class

(ii) The identity element of a gp being not conjugate to any other element forms a gp by itself since $x\bar{x}^1 = e$ $\forall x \in G$

(iii) Every element of an abelian gp is conjugate with itself since

$$ax = xa \quad \forall x \in G$$

$$\Rightarrow \bar{x}^1 ax = \bar{x}^1 xa$$

$$\bar{x}^1 ax = a \quad \forall x \in G$$

$$\Rightarrow a \sim a$$

$\Rightarrow$ The conjugacy class of an abelian gp consists of a single element

(iv) No class can be a subgp. unless it contains only the identity element e

(v) All elements of a conjugacy class have the same order.

Proof Let a be an element of a class. Then $\bar{x}^1 ax$ will also be one element of it

Let $o(a) = n$

$$\Rightarrow a^n = e$$

$$\therefore (\bar{x}^1 a x)^n = (\bar{x}^1 a x)(\bar{x}^1 a x)^{n-1}$$
$$= (\bar{x}^1 a x).\ \bar{x}^1 a x.(\bar{x}^1 a x)^{n-2}$$
$$= a^2 (\bar{x}^1 a x)^{n-2} \quad \text{---}$$
$$= a^4 (\bar{x}^1 a x)^{n-4}$$
$$= \text{---}$$
$$= a^n = e$$

$\Rightarrow$ order of $(\bar{x}^1 a x)$ is also n.

(Vi) If a single element of a class of a gp is given, then whole class may be determined e.g if the elements of a gp G_1 are $a_1, a_2, \text{---} a_n$. Then the class of G may be determined by forming the sequence

$$\bar{e}^1 a_1 e,\ \bar{a}_2^1 a_1 a_2 \text{ ---} \bar{a}_n^1 a_1 a_n$$

Evidently all these elements of the sequence are conjugate to one another and form a class.

(Vii) $C_a = C_b \Leftrightarrow a \sim b$

Theorem The number of elements in a conjugacy class C_a of an element a of G_1 is equal to the index of normalizer of a in G_1 i.e index of $N_{G_1}(a)$ in G_1

Proof: Let C be the collection of right cosets of the Normaliser $N_{G_1}(a) = N$ of $a \in G_1$.

We are to show that no of elements in C is equal to no of elements in C_a

Define a mapping

$$\varphi : C \longrightarrow C_a \text{ as}$$

$$\varphi(Ng) = \bar{g}^1 a g = \bar{g}^1 a (\bar{g}^1)^{-1}$$

The mapping φ is well defined because if $Ng = Ng'$

$$\Rightarrow g'\bar{g}^{-1} \in N$$

i.e $g'\bar{g}^{-1} = n$ for some $n \in N$

$\Rightarrow g' = ng$

example.

$\bar{g}^1 a g' = (ng)^{-1} a (ng) = \bar{g}^1 (n^{-1} a n) g$ $\quad \because n \in N_G(a)$
$= \bar{g}^1 a g$ $\quad \therefore an = na$
$\Rightarrow n^{-1} an = a$

Next let $gag^{-1} \in Ca$. Then $\varphi(Ng^{-1}) = gag^{-1}$ for $Ng^{-1} \in C$

So that φ is surjective.

let

$$\varphi(Ng) = \varphi(Ng')$$

we shall that $Ng = Ng'$

Now $\varphi(Ng) = \varphi(Ng')$

$\Rightarrow \bar{g}^1 a g = g'^{-1} a g'$

$\Rightarrow g' \bar{g}^{-1} a g g'^{-1} = a$

$\Rightarrow g' \bar{g}^{-1} a (g' \bar{g}^{-1})^{-1} = a \Rightarrow g' \bar{g}^{-1} a = a\, g' \bar{g}^{-1}$

$\Rightarrow g' \bar{g}^{-1} \in N$

$\Rightarrow g' \in Ng$

But $g' \in Ng'$

Hence $Ng = Ng'$

Thus φ is a bijection between C & Ca. So C & Ca have the same number of elements

Corollary: Let G be a finite gp. & $a \in G$. Then the number m of elements in Ca divides the order of the gp. i.e $|G| = (G : N_G(a))\, N_G(a)$

proof: The number m of elements in Ca is equal to the index of normaliser

$$N_G(a) = \{x \in G : xa = ax\}$$

of a in G.

But $N_G(a)$ is a sub-gp of G. So m being the index of $N_G(a)$ in G divides the order of G, by Lagrange's theorem

Remark Consider the class equation

$$n = m_1 + m_2 + \cdots + m_r$$

where m_i is the number of elements in the conjugacy class C_{a_i}; $i = 1, 2, \ldots, r$, $a_i \in G$

By the above corollary

$$m_i / n$$

If G is a gp and $Z \in \mathcal{Z}(G)$. Then

$$C_Z = \{Z\}$$

Since Z commute will all elements of G i.e

$$xZ = Zx \quad \forall x \in G$$

$$\Rightarrow xZx^{-1} = Z \quad \forall x \in G$$

$\Rightarrow Z$ is conjugate to itself

$\therefore C_Z = \{Z\}$ So $|C_Z| = 1$.

In particular if G is a abelian gp then for each $a \in G$

$$C_a = \{a\}$$

because G is abelian and

$$ax = xa \quad \forall x \in G$$

$$x^{-1}ax = a \quad \forall x \in G$$

$\Rightarrow$ a is only conjugate of a.

$\Rightarrow C_a = \{a\}$

Theorem: If G is a finite gp and $a \in G$, then

$$|C_a| = \frac{|G|}{|N_G(a)|} = \frac{o(G)}{o[N_G(a)]}$$ i.e order of C_a

is equal to quotient when $o(G)$ is divided by $o(N_G(a))$

Proof Let $o(G) = n$ and $N_G(a) = N$ has t distinct right cosets

$$Nx_1, Nx_2, \ldots, Nx_t$$

The by Lagrange's theorem we know that

$$t = \frac{o(G_1)}{o(N_{G_1}(a))}$$

Now, for $1 \le i, j \le t$ if

$$x_i^{-1} a x_i = x_j^{-1} a x_j$$

Then

$$\Rightarrow x_i x_j^{-1} a x_j x_i^{-1} = a$$

$$\Rightarrow x_i x_j^{-1} a (x_i x_j^{-1})^{-1} = a$$

$$\Rightarrow (x_i x_j^{-1}) a = a (x_i x_j^{-1})$$

$$\Rightarrow x_i x_j^{-1} \in N_{G_1}(a) = N$$

$$\Rightarrow N x_i = N x_j$$

$$\Rightarrow i = j$$

Since Nx_i's all distinct

Hence $x_i^{-1} a x_i = x_j^{-1} a x_j \Rightarrow i = j$

So $x_1^{-1} a x_1, x_2^{-1} a x_2 \dots\dots x_t^{-1} a x_t$ are all distinct conjugates of a

If we show that these are the only conjugates of a, then it follows that C_a contains only t-elements i.e

$$|C_a| = t = \frac{o(G_1)}{o(N_{G_1}(a))}$$

Consider for some $x \in G_1$

$$b = x^{-1} a x$$

Since $G_1 = \bigcup_{i=1}^{t} N_{G_1}(a) x_i = \bigcup_{i=1}^{t} N x_i$

$\therefore$ $x = c x_i$ for some $c \in N_{G_1}(a) = N$ & for some +ve integer i

Therefore

$$x^{-1} a x = (c x_i)^{-1} a (c x_i)$$

$$= x_i^{-1} (c^{-1} a c) x_i \quad \left| \because c \in N_{G_1}(a) \Rightarrow ac = ca \Rightarrow c^{-1} a c = a \right.$$

$$= x_i^{-1} a x_i$$

Hence any conjugate b of a is equal to one of $x_i^{-1} a x_i$

$\Rightarrow$ a has only t conjugates viz $x_i^{-1} a x_i$, $i = 1, 2, \dots t$

Thus $|Ca| = t = \dfrac{o(G)}{o[N_G(a)]}$

Corollary 1 For any finite gp G, $o(G) = \sum_a \dfrac{o(G)}{o[N_G(a)]}$ where sum runs over a, taken one each from each conjugate class.

i.e $|G| = \dfrac{o(G)}{o(N(a_1))} + \dfrac{o(G)}{o(N(a_2))} + \cdots \dfrac{o(G)}{o(N(a_n))}$

Proof where $a_1, a_2, \ldots a_k$ belong to $Ca_1, Ca_2 \ldots Ca_k$

Let $Ca_1, Ca_2, \ldots Ca_k$ be the totality of conjugate classes in G.

Then the fact these classes are pairwise disjoint and their union is G gives

$$o(G) = |G| = \sum_{i=1}^{k} |Ca_i| \quad , \text{where } |Ca_i| = o(Ca_i)$$

But by above theorem

$$|Ca_i| = \frac{o(G)}{o[N_G(a_i)]}$$

Hence $$|G| = \sum_{i=1}^{k} \frac{o(G)}{o[N_G(a_i)]}$$

$$= \sum_a \frac{o(G)}{o[N_G(a)]}$$

where a is taken one each from each Conjugate class.

Corollary 2: Let G be a finite gp and $f(G)$, its centre, then (Plus)

$$o(G) = o[f(G)] + \sum_a \frac{o(G)}{o[N_G(a)]}$$ where

the sum sums over elements a, taken one from each of those distinct conjugate classes which more than one element.

Proof: Since $a \in f(G)$ iff $|Ca| = 1$

∴ There are ~~orders~~ of $o[f(G)]$

number of conjugate classes ~~which~~ each having only one element. Therefore the corollary follows.

Def Let G be a finite gp. The equation

$$o(G) = o[f(G)] + \sum_{a} \frac{o(G)}{o[N_G(a)]}$$ where the sum

runs over elements a, taken on from each of those distinct conjugate classes which contain more than one element, is called class equation of the gp G

Class equation plays an important role in the structure theory of non-commutative finite groups.

Theorem (a) Let G be a gp., $a, b, c \in G$. Then if a is conjugate with b and c both, b & c are conjug with each other

(b) Two elements x & y transform an element a, alike iff they belong to the same right coset of the normaliser $N_G(a)$ of a in G.

Proof (a) Given that

$$a \sim b \;\&\; a \sim c$$

$$\Rightarrow a = \bar{x}^1 b x \text{ and } a = \bar{y}^1 c y \text{ for some } x, y \in G$$

$$\Rightarrow \bar{x}^1 b x = \bar{y}^1 c y$$

$$\Rightarrow x(\bar{x}^1 b x) = x(\bar{y}^1 c y)$$

$$\Rightarrow (x\bar{y}^1)(cy)$$

$$\Rightarrow (bx)\bar{x}^1 = (x\bar{y}^1)(cy)\bar{x}^1$$

$$\Rightarrow b = x\bar{y}^1 c y \bar{x}^1$$

$$= (x\bar{y}^1)\, c\, (x\bar{y}^1)^{-1}$$

Now since $x, y \in G \Rightarrow \bar{x}^1, \bar{y}^1 \in G \Rightarrow x\bar{y}^1 \in G$

Hence $b \sim c$ i.e b is conjugate to c

(b) Suppose that two elements x, y of G are such that they transform, a, alike so that

$$x^{-1}ax = y^{-1}ay$$

$$\Rightarrow \quad yx^{-1}a = ayx^{-1}$$

$$\Rightarrow \quad yx^{-1}a = ayx^{-1}$$

$$\Rightarrow \quad yx^{-1} \in N_G(a) \Rightarrow yx^{-1}N_G(a) = N_G(a)$$

& $N_G(a)\, yx^{-1} = N_G(a)$

$$\Rightarrow \quad N_G(a)\, x = N_G(a)\, y$$

Thus two elements which transform an element 'a, alike belong to the same right coset of the normaliser $N_G(a)$

Conversely let $x \in N_G(a)$, $y \in N_G(a)$

$$\Rightarrow \quad xa = ax \quad \text{and} \quad ya = ay$$

we have

$$ay = ya$$

$$\Rightarrow \quad y^{-1}a = ay^{-1}$$

$$\Rightarrow \quad x(y^{-1}a) = x(ay^{-1})$$

$$\Rightarrow \quad (xy^{-1})a = (xa)y^{-1} = (ax)y^{-1} = a(xy^{-1})$$

Conversely let $z \in N_G(a)$

so that $zx \in N_G(a)x$

we have

$$(zx)^{-1}a(zx) = x^{-1}(z^{-1}az)x = x^{-1}ax$$

So that each element of $N_G(a)x$ transforms as x does.

Self Conjugate Elements (invariant or Central)

An element $a \in G$ is said to be self-conjugate if a is the only member of conjugacy class C_a of elements conjugate to a.

Thus a, is self-conjugate iff

$$a = x^{-1}ax \quad \forall x \in G$$

$$\Leftrightarrow xa = ax \quad \forall x \in G$$

i.e a commutes with every element of G.

$\Rightarrow a \in$ centre of G. Hence a is self-conjugate iff $a \in \zeta(G)$.

Thus a self-conjugate element of gp may be defined as one which commutes with each element of the group i.e it belongs to centre of that gp.

Remark In case of abelian gp, no two elements are conjugate and there are as many conjugacy classes as the number of elements in that gp. Thus in abelian gp every element is self-conjugate.

Theorem The set Z of all self-conjugate elements of a group G is a sub-group of the group.

Proof Let $a, b \in Z$ so that

$$ax = xa \quad bx = xb \quad \forall x \in G.$$

Now

$$bx = xb \quad \forall x \in G$$

$$\Rightarrow xb^{-1} = b^{-1}x \quad \forall x \in G.$$

$$(ab^{-1})x = a(b^{-1}x) = a(xb^{-1}) = (ax)b^{-1}$$

$$= (xa)b^{-1} = x(ab^{-1}) \quad \forall x \in G.$$

$$\Rightarrow ab^{-1} \in Z$$

$\Rightarrow Z$ is a subgroup of G

Centre of gp

The set of all self-conjugate elements of a gp is called the centre or central of the gp

Problem Show that the normaliser of a self-conjugate element of a gp is the gp itself.

Solution Let G be a gp. and a, be its self-conjugate element.

Then

$$ax = xa \quad \forall x \in G$$

$\Rightarrow$ Every element of G belongs to $N_G(a)$

Hence $N_G(a) = G$.

Problem Show that $N_G(a) \supseteq gp(a) = \langle a \rangle$ $N_G(a)$ being the normaliser of a and $gp(a)$ denoting the cyclic gp. generated by a

Solution Since $aa^k = a^k a$ for any integer k

$\Rightarrow$ $N_G(a)$ contains together with a all powers of a

Hence $N_G(a) \supseteq gp(a)$ (completed)

Conjugate Complexes & Conjugate Complexes & Conjugate Subgroups

Conjugate Complexes Let K & L be two complexes of a gp. G. Then K is conjugate to the complex L if $\exists$ an element $x \in G$, such that

$$K = xLx^{-1}$$

Here $xLx^{-1} = \{xax^{-1} : a \in L\}$

Remark It may be shown that this relation of Conjugacy is an equivalence relation. Therefore the set of all complexes can be partitioned into mutually disjoint classes of pairwise Conjugate Complexes.

Theorem (Conjugate subgroup)

Let H be a subgroup of a gp. G. Then for any $x \in G$, the set

$xHx^{-1} = \{xhx^{-1} : h \in H\}$ is a subgroup of G and is called a Conjugate subgroup to H in G.

OR

Each complex conjugate to a sub-group is a a sub-group.

Proof Let $K = xHx^{-1} = \{xhx^{-1} : h \in H\}$, & $k_1, k_2 \in K$. Then

$k_1 = xh_1x^{-1}$ $\quad k_2 = xh_2x^{-1}$ $\quad h_1, h_2 \in H$

So $k_1k_2^{-1} = (xh_1x^{-1})(xh_2x^{-1})^{-1}$

$= (xh_1x^{-1})(xh_2^{-1}x^{-1})$

$= xh_1(x^{-1}x)h_2^{-1}x^{-1}$

$= x(h_1h_2^{-1})x^{-1}$

$= xh_3x^{-1} \in K$ $\quad h_1h_2^{-1} = h_3 \in h$

$\Rightarrow k_1k_2^{-1} \in K$. Therefor K is a subgp. of G

Theorem Relation of Conjugacy between the subgroups of a group is an equivalence relation.

Proof

(a) Reflexivity Let H & K be subgroups of a groups, then

$H = eHe^{-1}$ } where e is the identity
or $K = eKe^{-1}$] element of G.

$\Rightarrow H \sim H$

$\Rightarrow$ Reflexive property holds

(b) Symmetry Let H & K be subgroups of G such that $H \sim K$

Then there exists ax $x \in G$, s.t

$H = xKx^{-1}$

so $K = x^{-1} H (x^{-1})^{-1}$

$\Rightarrow K \sim H$

Therefore relation of Conjugacy is symmetric

(c) Transitivity

Let H, K, M be subgroups of G. and $H \sim K$, $K \sim M$. Then $\exists$ elements $x, y \in G$ s.t

$K = xHx^{-1}$ $M = yKy^{-1}$

$M = yKy^{-1} = y(xHx^{-1})y^{-1} = yxH(yx)^{-1}$

$\Rightarrow H \sim M$

So $\sim$ is transitive. Hence is an equivalence relation.

Theorem: Any two Conjugate subgroups of a gp G are isomorphic.

Proof Let H & K be subgroups of G s.t that

$K = gHg^{-1}$ $g \in G$.

We show that H is isomorphic to K ($H \cong K$)

For this define a mapping $\varphi : H \longrightarrow K$ as follows

$\varphi(h) = ghg^{-1} \in K \quad \forall h \in H$

Then φ is injective because for $h_1, h_2 \in H$

$$\varphi(h_1) = \varphi(h_2)$$
$$\Rightarrow \quad g h_1 \bar{g}^1 = g h_2 \bar{g}^1$$
$$\Rightarrow \quad h_1 = h_2$$

Also for each $k = gh\bar{g}^1$ in K, $h \in H$ is the image of $h \in H$ under φ. So φ is surjective.

Lastly for $h_1, h_2 \in H$

$$\varphi(h_1 h_2) = g\, h_1 h_2 \bar{g}^1$$
$$= g h_1 \bar{g}^1 g\, h_2 \bar{g}^1$$
$$= \varphi(h_1)\, \varphi(h_2)$$

$\Rightarrow \varphi$ is homomorphism.

So φ is isomorphism between H & K.

i.e $H \cong K$.

Cor: Any two conjugate subgroups of a subgroup G have the same order.

Proof Let H & K be conjugate subgroups of G. Then

$H \cong K$ (by the above theorem)

As there is bijective mapping in H & K. So H & K have the same no. of elements.

Conjugacy class of a Sub-group

Let H be a subgroup of a group G. The collection of all those subgroups of G which are conjugate to H is denoted by C_H and is called the conjugacy class of H. Thus

$$C_H = \{ K \subseteq G : K = gH\bar{g}^1 \text{ for some } g \in G \}$$

Theorem The number of elements in the conjugacy class C_H determined by a sub-group H of G is equal to the index of the normaliser of H in G.

Proof Let C be the all right cosets of normaliser $N_G(H) = N$ of H in G. Then the number of elements in C is equal to the index of N in G.

Define a mapping $\varphi : C \longrightarrow C_H$ as

Let $Ng \in C$, $g \in G$ we put

$$\varphi(Ng) = \bar{g}^1 H (\bar{g}^1)^{-1} = \bar{g}^1 H g$$

First we show that φ is well defined

For this let $Ng = Ng'$, $g, g' \in G$

Then $Ng\bar{g}'^{-1} = N \Rightarrow g\bar{g}' \in N$

so that $g\bar{g}'^{-1} = n$, $n \in N$

i.e. $g' = ng$

Hence

$$\varphi(Ng') = \bar{g}'^{-1} H g' = (ng)^{-1} H (ng)$$

$$= \bar{g}^1 (\bar{n}^1 H n) g \qquad (\because n \in N \Rightarrow nH = Hn \Rightarrow H = \bar{n}^1 H n)$$

$$= \bar{g}^1 H g = \varphi(Ng)$$

Next let $x H \bar{x}^1 \in C_H$

Then $\varphi(Nx\bar{x}^1) = x H \bar{x}^1$ for $Nx^{-1} \in C_H$

$\Rightarrow \varphi$ is surjective

Again to show that φ is injective

Let $\varphi(Ng) = \varphi(Ng')$

$\Rightarrow \bar{g}^1 H g = \bar{g}'^{-1} H g'$

$\Rightarrow g'\bar{g}^{-1} H g \bar{g}'^{-1} = H$

$\Rightarrow (g'\bar{g}^{-1}) H (g'\bar{g}^{-1})^{-1} = H$

$\Rightarrow g'\bar{g}^{-1} H = H g'\bar{g}^{-1}$

$\Rightarrow g'\bar{g}^{-1} \in N = N_G(H)$

$\Rightarrow gg'^{-1}N = N$

$\Rightarrow g' \in Ng$ But $g' \in Ng'$

Hence $Ng = Ng'$

Thus ϕ is a bijection between C & C_H

So C & C_H have the same number of elements

Problem Let $G_1 = \langle a, b : a^4 = b^2 = (ab)^2 = 1 \rangle$

(This group is called dihedral group of order 8)

(i) Write all the elements (ii) Find all the sub-gps. of G_1 (iii) Which of these are conjugate to each other

Solution If $G_1 = \langle a, b : a^4 = b^2 = (ab)^2 = 1 \rangle$

(i) Then all its elements are. order $= 4 \times 2 = 8$

$1, a, a^2, a^3, b, ab, a^2b, a^3b$

From $(ab)^2 = 1$

$abab = 1$ we have $\boxed{\begin{array}{l} ba = a^3b \\ ab = ba^3 \end{array}}$

Using this and the given relation we can show that every other element of G_1 is one the elements listed above

e.g $ba^2ba = ba^2a^3b = ba^5b$

$= babb = a^3bb = a^3 \in G_1$

Similarly a^2ba^3b

(ii) The sub-groups of G_1 are

$H_4 = \{1\}$ $H_2 = \langle a : a^4 = 1 \rangle = \{1, a, a^2, a^3\}$ $\because a^4 = 1$

$H_3 = \{1, a^2 : a^4 = 1\}$

	1	a^2
1	1	a^2
a^2	a^2	1

$H_4 = \langle b : b^2 = 1 \rangle = \{1, b\}$

$H_5 = \{1, ab\}$, $H_6 = \{1, a^2b\}$ with $(a^2b)^2 = a^2ba^2b$

$= a^2baab$

$= a^2a^3bab$

$= abbab$

$= aa^3bb$

$= b^2 = 1$

order of H_6 is 2 ($a^2 = 1$, $a^2 = 1$)

$H_7 = \{1, a^3b\}$ $a^3b \cdot a^3b = ba\,a^3b$

$= b^2 = 1$

$H_8 = \langle a^2, b : a^4 = 1, b^2 = 1, a^2b = ba^2 \rangle$

$= \{1, a^2, b, a^2b\}$

$Hq = G$

$ba^2 = ba \cdot a$

$= a^2ba$

$= a^3 \cdot a^3b = a^2b$

or $a^4b = a \cdot ab = aba^3$

$= ba^3 \cdot a^3 = ba^2$.

iii

Normal or Self-Conjugate Sub-groups

Before defining normal sub-group we prove a theorem

Theorem: Let H be a sub-group of a gp G. Then $gH = Hg$ for all $g \in G$ iff $ghg^{-1} \in H$ for all $h \in H$ and for all $g \in G$ i.e iff every conjugate of all elements of H in G is in H

Proof: Let $gH = Hg \quad \forall g \in G$

Then for each $h \in H$, $hg = gh_1$ for some $h_1 \in H$

$\Rightarrow g^{-1}hg = h_1 \in H$ for each $h \in H$

OR Let $gH = Hg \quad \forall g \in G$

Then for each $h \in H$, $gh = h_1 g$ for some $h_1 \in H$

$\Rightarrow ghg^{-1} = h_1 \in H$ for each $h \in H$

$\Rightarrow ghg^{-1} \in H$ for each $h \in H$, for all $g \in G$

Conversely Let $ghg^{-1} \in H \quad \forall h \in H, \forall g \in G$

$\Rightarrow ghg^{-1} = h_1$ for some $h_1 \in H$

$\Rightarrow gh = h_1 g$

$\Rightarrow gh \in Hg \quad \forall h \in H, \forall g \in G$

$\Rightarrow gH \subseteq Hg \longrightarrow (A)$

Let $hg \in Hg$

Then $hg = (gg^{-1})hg = g(g^{-1}hg)$

$= g(g^{-1}h(g^{-1})^{-1}) \in gH$

$\because g^{-1}h(g^{-1})^{-1} \in H$ by given condition

$\Rightarrow hg \in gH$

$\Rightarrow Hg \subseteq gH \longrightarrow (B)$

By (A) & (B) we have

$gH = Hg$

Normal Sub-group (Normal divisor or invariant sub-gp or self-Conjugate sub-gp)

A sub-gp H of a gp G is normal in G if $ghg^{-1} \in H$ for all $g \in G$ and for all $h \in H$.
Symbolically it is denoted by $H \triangle G$ or $G \triangleleft H$ or $H \triangle G$
OR By above theorem H is normal in G iff $gH = Hg$ (equivalently $gHg^{-1} = H$)

Remarks
- For a gp G, G and $\{e\}$ are always normal subgroups of G and these sub-groups are Called trivial normal subgroups or improper normal subgroups. Normal sub-gps of G which are different from these two are called proper normal subgroups.
- Every subgroup of an abelian gp is a normal Sub-group.
- The relation of "being normal ~~to~~ subgp" is not transitive. Thus if $H \triangleleft K$ & $K \triangle G$, then H may not be a normal subgp of G.

Hamiltonian gp A non-abelian gp all of whose sub-gps are normal is called Hamiltonian gp.

Simple gp A gp having no non-trivial (proper) sub-gp is called simple gp.

Theorem A sub-gp of G is normal in G iff $gHg^{-1} = H$ for all $g \in G$ i.e iff H is self-Conjugate.

Proof Suppose that H is normal in G. Then
for any $h \in H$, $g \in G$, $ghg^{-1} \in H$
To show that $gHg^{-1} = H$ for all $g \in G$
Let $ghg^{-1} \in gHg^{-1}$ for $h \in H$
Since H is normal in G
$\therefore ghg^{-1} \in H$
Hence $gHg^{-1} \subseteq H$ ——→ (1)
Let $h \in gHg^{-1}$, then $g^{-1}h(g^{-1})^{-1} \in H$ ($\because H \triangleleft G$)
so $h = gg^{-1}h(g^{-1})^{-1}g^{-1} = gh'g^{-1} \in gHg^{-1}$ $h' = g^{-1}h(g^{-1})^{-1} \in H$
Hence $H \subseteq gHg^{-1}$ ——→ (2)

From ① & ②

$$H = gHg^{-1}$$

Conversely

Suppose that, for any $g \in G$, $gHg^{-1} = H$

Then for any $h \in H$, $g \in G$, $ghg^{-1} \in gHg^{-1} = H$

So H is normal in G.

Theorem (Cor) A sub-gp H of G is normal in G iff $gH = Hg \quad \forall g \in G$

Proof Since H is normal in G

$$\Leftrightarrow gHg^{-1} = H \quad \forall g \in G$$
$$\Leftrightarrow gH = Hg \quad \forall g \in G$$

Examples

1) The subgroup $H = \langle \phi : \phi^3 = e \rangle$ is a normal sub-gp of the gp $G = \langle \phi, \psi : \phi^3 = \psi^2 = (\phi\psi)^2 = e \rangle$

Here $G = \{e, \phi, \phi^2, \psi, \phi\psi, \phi^2\psi\}$

$$H = \{\phi, \phi^2, e\}$$

$eHe^{-1} = \{\phi, \phi^2, e\} = H$

$\phi H\phi^{-1} = \{\phi, \phi^2, e\} = H$

$\phi^2 H\phi^{-2} = \{\phi^2\phi\phi^{-2}, \phi^2\phi^2\phi^{-2}, \phi^2 e\phi^{-2}\}$

$= \{\phi, \phi^2, e\} = H$

$\psi H\psi^{-1} = \{\psi\phi\psi^{-1}, \psi\phi^2\psi^{-1}, \psi e\psi^{-1}\}$

$= \{\psi\phi\psi, \psi\phi^2\psi, e\}$

$= \{\phi^2\psi\psi \quad \phi\psi\psi, e\}$

$= \{\phi^2 \quad \phi, e\} = H$

$\phi\psi \cdot \phi\psi = e$.

$\phi\psi = \psi^{-1}\phi^{-1} = \psi\phi^2$

$\phi^2 = e$

$\Rightarrow \psi = \psi^{-1}$

$\phi^{-1} = \phi^2$

$\phi\psi H(\phi\psi)^{-1} = \{\phi\psi\phi(\phi\psi)^{-1}, \phi\psi\phi^2(\phi\psi)^{-1}, e\}$

$= \{\phi\psi\phi\phi\psi, \phi\psi\phi^2\phi\psi, e\}$

$= \{\phi\psi\phi^2\psi \quad \phi\psi\phi^3\psi, e\}$

$= \{\phi\psi\psi\phi \quad \phi\psi^2 \quad e\} = \{\phi^2, \phi, e\} = H$

Also $(\phi^2\psi)^3 H (\phi^2\psi)^{-1} = H$

Hence $H \triangleleft G$.

2) Let $G = \langle a, b, c : a^3 = b^2 = c^2 = (bc)^2 = 1, ab = ca, ac = bca \rangle$ Then the sub-gp $K = \langle b, c : b^2 = c^2 = (bc)^2 = 1 \rangle$ is normal in G. Also the gp $H = \langle b : b^2 = 1 \rangle$ is normal k. However H is not a normal sub-gp in G because

$$aHa^{-1} = \{1, aba^{-1} = c\} \neq H$$

3) The group of quaternians $\pm I, \pm i, \pm j, \pm k$ is such that it is non-abelian but every sub-gp of Q is normal in Q

4) A cyclic group C whose order is a prime number is simple. In this case C, by Lagrange's theorem, has no proper sub-groups and therefore no proper normal subgroups. The class of cyclic groups of prime order is the only class of abelian simple gp.

Theorem (Properties of normal sub-groups)

(a) Every subgroup of an abelian gp. is normal subgp.

(b) The right and left coset decompositions of a gp relative to normal subgroup are same.

(c) Every element conjugate to an element of a normal sub group is an element of the sub-group i.e if H is normal sub-gp, then

$$a \in H \Rightarrow C_a \subseteq H$$

(d) The intersection of any two normal subgroups of a group is normal sub-group

Proof (a) Let H be an abelian sub-gp of G. Then

$$gH = Hg \quad \forall g \in G$$

$$\Rightarrow H \triangleleft G$$

or Then $hg = gh \quad \forall h \in H, \forall g \in G$

$$h = ghg^{-1} \in H \quad \forall h \in H \quad \forall g \in G$$

$$\Rightarrow H \triangleleft G$$

(b) Since for a normal sub-gp H of G

$$gH = Hg \quad \forall g \in G$$

Therefore right and left coset decompositions of G relative H are are same

(c) Let $H \triangleleft G$

Then

$\Leftrightarrow gHg^{-1} = H \quad \forall g \in G$

$\Leftrightarrow ghg^{-1} \in H \quad \forall g \in G, \forall h \in H$

$\Rightarrow$ Conjugate of every element of H is in H

Now if $a \in H$

Then every element conjugate to a is in H

$\Rightarrow C_a \subseteq H$

(d) Let H & K be two normal sub-groups of G.

Since $e \in H \cap K$, $H \cap K \neq \phi$

Now $a \in H \cap K$

$\Rightarrow a \in H$ and $a \in K$

But H & K are normal in G

$\therefore xa\bar{x}^1 \in H$ and $xa\bar{x}^1 \in K \quad \forall x \in G$.

$\Rightarrow xa\bar{x}^1 \in H \cap K \quad \forall x \in G$

$\Rightarrow H \cap K$ is normal sub-gp.

Theorem The intersection of any number of normal sub-groups of a group G is normal in G

Proof Let $\{H_\alpha : \alpha \in \Omega\}$ be any collection of normal sub-groups of a gp G.

Let $H = \bigcap_{\alpha \in \Omega} H_\alpha$

We show that H is normal in G.

Let $h \in H$ & $g \in G$

Then $h \in H_\alpha, \forall \alpha \in \Omega$

Since each H_α is normal in G

So $ghg^{-1} \in H_\alpha, \forall \alpha \in \Omega, \forall g \in G$

Hence $ghg^{-1} \in \bigcap_{\alpha \in \Omega} H_\alpha = H$

So H is normal in G.

Theorem (a) The centre of group G_1 is a normal subgroup of G_1

(b) The ~~centraliser~~ $C_{G_1}(H)$ of a complex H in is normal in $C_{G_1}(H)$, if H is an abelian sub-group

(c) If H is a sub-group of G_1, ~~H is normal~~ the normaliser $N_{G_1}(H)$ is normaliser of H in G_1. Then H is normal in $N_{G_1}(H)$. i.e. Every sub-gp of G_1 is normal in its own normaliser in G_1.

Proof (a) We have already proved that centre of gp is a sub-gp of that G_1. Now we prove that centre is normal

Let $\zeta(G_1) = C_{G_1}(G_1) = \{g \in G_1 : gx = xg \quad \forall x, g \in G_1\}$

If $g \in G_1$, $x \in \zeta(G_1)$

Then $gx = xg$

so $x = gxg^{-1} \in \zeta(G_1)$

$\because x$ & g are arbitrary

$\therefore gxg^{-1} \in \zeta(G_1) \quad \forall x \in \zeta(G_1)$ & $g \in G_1$

Thus $\zeta(G_1)$ is normal in G_1

(b) ~~Centraliser of an~~ abelian sub-gp H of G_1 is normal in its ~~itself~~ centraliser $C_{G_1}(H)$

Since $e \in C_{G_1}(H)$

$\therefore C_{G_1}(H) \neq \phi$

Since H is abelian gp

$\therefore$ each $h \in H$ belongs to $C_{G_1}(H)$

Now if $g \in C_{G_1}(H)$

then for each $h \in H$, $gh = hg$

$\Rightarrow h = ghg^{-1} \in H$

$\Rightarrow H$ is normal sub-gp of $C_{G_1}(H)$

($\subseteq$) Any sub-gp H of G_1 is normal in its normaliser $N_{G_1}(H)$ in G_1. Further if H is a sub-group of G_1, then H is normal sub-gp of G_1 iff $N_{G_1}(H) = G_1$

$N_{G_1}(H) = \{ g \in G_1 : gH = Hg \} \neq \phi \because e \in N_{G_1}(H)$

Since for every element g in $N_{G_1}(H)$, $gH = Hg$.

$\therefore H$ is normal in $N_{G_1}(H)$

Let $f, g \in N_{G_1}(H)$

then

$gH = Hg$ and $fH = Hf$

$\Rightarrow \bar{g}^1 H = H\bar{g}^1$ and $\bar{f}^1 H = H\bar{f}^1$

| $\because$ If H is subset of G_1
| $\& \; gH = Hg$
| $= \bar{g}^1 H = H\bar{g}^{-1}$

Now,

$(f\bar{g}^{-1})H = f(\bar{g}^1 H) = f(H\bar{g}^1) = (fH)\bar{g}^1$

$= (Hf)\bar{g}^1 = H(f\bar{g}^{-1})$

| $(fg)H = f(gH)$
| $H(fg) = (Hf)g$
| $(fH)g = f(Hg)$
| for $f, g \in G_1$

$\Rightarrow N_{G_1}(H)$ is sub-group of G_1.

Clearly if H is a sub-gp, then $H \subseteq N_{G_1}(H)$ and $H \trianglelefteq N_{G_1}(H)$

Now if H is a sub-gp and $H \trianglelefteq G_1$, then for each each $g \in G_1$, $gH = Hg$

Hence $g \in N_{G_1}(H)$

So $G_1 \subseteq N_{G_1}(H)$

But $N_{G_1}(H) \subseteq G_1$

$\Rightarrow N_{G_1}(H) = G_1$

If H is a sub-gp and $N_{G_1}(H) = G_1$. Then

Since $H \trianglelefteq N_{G_1}(H) = G_1$

$\Rightarrow gH = Hg \; \forall \; g \in N_{G_1}(H) = G_1$

$\Rightarrow H \trianglelefteq G_1$

Theorem If H & K are sub-gps of a G_1 such that H is normal in G_1, then $H \cap K$ is normal in K

Proof: Let H be normal in G_1. Let $x \in K, a \in H \cap K$

Then $xax^{-1} \in K$ ($\because x, a \in K$ & K is sub-gp)

Further $xax^{-1} \in H$ Since H is normal and $a \in H, x \in K \subseteq G_1$

$\Rightarrow xax^{-1} \in H \cap K \quad \forall x \in K, a \in H \cap K$

Hence $H \cap K$ is normal subgp of K

Theorem H is normal sub-group of G_1 and K is a sub-group of G_1 such that

$H \subset K \subset G_1$

Then H is also a normal subgroup of K

Proof Since H is normal in G_1

$\Rightarrow gH = Hg \quad \forall g \in G_1$

But $K \subset G_1$

$\Rightarrow xH = Hx \quad \forall x \in K$

$\Rightarrow$ H is normal in K

Theorem If H & K are ~~normal~~ sub-groups of G_1, then

(a) HK is a normal sub-gp of G_1 if either H or K is normal in G_1

(b) HK is a normal sub-gp of G_1 iff H and K are both normal in G_1.

Proof (a) Since HK is a sub-group of G_1 iff

$HK = KH$

Therefore if H is a normal sub-gp of G_1. Then

$HK = kH \quad \forall k \in K$

$\Rightarrow HK = KH$

$\Rightarrow$ HK is a sub-gp of G_1

Similarly if K is normal then $hK = kh \ \forall \ h \in H$

$\Rightarrow HK = KH$

$\Rightarrow$ HK is ~~normal~~ sub-gp

OR Let K is normal in G_1

$HK = \{x \mid x = hk, h \in H, k \in K\}$

$HK \neq \phi$ as $e \cdot e = e \in HK$

Let $g_1, g_2 \in HK$

$\Rightarrow g_1 = h_1k_1 \quad g_2 = h_2k_2$ where $h_1, h_2 \in H$ & $k_1, k_2 \in K$

Now $g_1 g_2^{-1} = h_1 k_1 (h_2 k_2)^{-1} = h_1 k_1 k_2^{-1} h_2^{-1}$

$= h_1 k_3 h_2^{-1}$ where $k_3 = k_1 k_2^{-1} \in K$

$= h_1 h_2^{-1} h_2 k_3 h_2^{-1}$

$= h_1 h_2^{-1} (h_2^{-1})^{-1} k_3 (h_2^{-1})$

$= a\,b$, say

where $a = h_1 h_2^{-1} \in H$ & $b = (h_2^{-1})^{-1} k_3 h_2^{-1} \in K$ as $K \trianglelefteq G$.

Thus $g_1 g_2^{-1} \in HK$

$\Rightarrow$ HK is a sub-gp

(b)

$HK \neq \phi$ as $e = e \cdot e \in HK$

First we show that HK is a sub-gp (proved above)

Let $g_1, g_2 \in HK$

$\Rightarrow g_1 = h_1 k_1 \qquad g_2 = h_2 k_2$

Now $g_1 g_2^{-1} = h_1 k_1 k_2^{-1} h_2^{-1}$

$= h_1 k_3 h_2^{-1}$ where $k_3 = k_1 k_2^{-1} \in K$

$= h_1 k_3 h_2^{-1}$

$= h_1 k_3 h_1^{-1} h_1 h_2^{-1} = h_1 h_2^{-1} h_2 k_3 h_2^{-1}$

$\because$ H & K are normal sub-gp

$\therefore$ $h_1 h_2^{-1} \in H$ ($\because$ H is sub-gp)

& $h_2 k_3 h_2^{-1} \in K$ as $K \trianglelefteq G_1$

$\Rightarrow g_1 g_2^{-1} \in HK$

$\Rightarrow$ HK is ~~normal~~ sub-gp

Next we prove that HK is normal in G_1

Since H is normal in G_1

$\Rightarrow g h g^{-1} \in H \quad \forall\, h \in H, \forall\, g \in G_1$

Also since K is normal

$\therefore g_1 k g_1^{-1} \in K \quad \forall\, k \in K, \forall\, g_1 \in G_1$

$\Rightarrow$ ~~$(ghg^{-1})(gkg^{-1})$~~

let $hk \in HK$ and $g \in G_1$

Then $g hk g^{-1} = g h g^{-1} g k g^{-1} \in HK$

$\because g h g^{-1} \in H \ \forall\, g \in G_1, \forall\, h \in H$

$\Rightarrow g hk g^{-1} \in HK \ \forall\, g \in G_1$ & $\forall\, hk \in HK$

& $g k g^{-1} \in K \ \forall\, g \in G_1, \forall\, k \in K$

Hence HK is normal in G.

Theorem:- If p the smallest prime factor of the order a finite grp, prove that any sub-gp of index p is normal

Proof:- ~~First prove that if $x \notin$~~

Let H be sub-gp of G, of index p

First we pr that if $x \notin H$, then

$x^i \notin H \quad \forall\ i = 1, 2, \ldots p-1$

If it is not trthen we can find $1 < k \leq p-1$ such that $x^k \in$

Let j be the leeve integer such that $x^j \in H$

in other words $\notin H$ for $t = 1, 2, \ldots j-1$

Let $o(x) = n$ and $o(G) = m$

As n/m and $< j < p$ and p is smallest factor of m, we get that can not divide n so there exist $q, r \in Z$ such it

$m = qj + r \quad 0 < r < j$

$\because o(x) = n \quad \therefore x^m = e$

$\Rightarrow x^{qj+r} = e$

$\Rightarrow (x^j)^q x^r = e$

$\Rightarrow (x^j)^{-q} = x^r$

$\Rightarrow x^r \in H$ as $x^j \in H$

If $j \mid m$
Then $j \mid m$
But p is
factor
$\therefore j \nmid m$

This violates the choice of j. Hence our supposition is true.

Now let H is nt normal in G

Then $\exists$ some $x \in G, h \in H$ such that

$x^{-1}hx \notin H$

$\Rightarrow hx \notin xH \quad x \notin H$ since if $x \in H$, then $x^{-1}h$ must be in H as H is sub

Set $He = H, Hx, Hx^2 \ldots Hx^{p-1}$ be the right coset of H. We prove that these are distinct

For this let

$Hx^i = Hx^j$ for $1 \leq i < j \leq p-1$

λ Let $y = x^{-1}hx$ then as $y \notin$ a similar fashion we get

$\Rightarrow x^i = h_i x^j$ for some $h_i \in H$

$\Rightarrow x^{i-j} = h_1 \in H$

$\Rightarrow x^{j-i} = h_1^{-1} \in H$.

which is contradiction to choice of j.

Hence $H, Hx, \ldots \ldots Hx^{p-1}$ are the distinct right cosets of H. Similarly we get $H, Hy, Hy^2, \ldots Hy^{p-1}$ are distinct.

So the two sets $\{H, Hx, Hx^2 \ldots Hx^{p-1}\}$ and $\{H, Hy, Hy^2, \ldots Hy^{p-1}\}$ are equal

Thus $Hx = Hy^l \quad 1 \leq l \leq p-1$

$\Rightarrow x = h' y^l$ for some $h' \in H$

$\Rightarrow x = h' x^{pl} (x^{-1} h x)^l = h' h^l x \quad \because (x^{-1} h x)^n = x^{-1} h^n x$

$\Rightarrow h' x^{-1} = h^{-l}$

$\Rightarrow h^l h' = x$

$\Rightarrow x \in H$ as $h^l h \in H$

which is a contradiction

Hence H is a normal sub- of G.

Theorem Any sub-gp of index 2 in G is normal in G

Proof Let H be a subgp of index 2 in G.

Let $g \in G$. If $g \in H$ then

$$gH = H = Hg$$

and H is normal.

If $g \notin H$ then $H \neq gH$, $G = H \cup gH$ such that $H \cap gH = \{\} = \phi$

Similarly $H \cap Hg = \{\}$ and $G = H \cup Hg$

$\Rightarrow H \cup gH = H \cup Hg$

$\Rightarrow gH = Hg$.

OR

Since H is of index 2 in G

$\therefore G = H \cup xH = H \cup Hx \quad x \in G \sim H$

So $xH = Hx$ for $x \in G \sim H$

Now let $g \in G$, Then either $g \in H$ or $g \in xH$

If $g \in H$, then

$$gH = H = Hg \quad \because g \in H$$

If $g \in xH$. Then $g = xh$ for some $h \in H$

So $gH = (xh)H = x(hH) = (xH)h$

$= (Hx)h = H(xh) = Hg$

Thus H is normal.

OR

Let $g \in G$. Then if $g \in H$, $g^2 \in H$ as H is sub-

If $g \notin H$. Consider gH.

Since G has two distinct left cosets namely H, gH

If $g^2H = gH \Rightarrow gH = H \Rightarrow g \in H$, a contradiction

So $g^2H = H \Rightarrow g^2 \in H$

Hence H is normal in G

Theorem If H is a sub-gp of G such that $g^2 \in H \ \forall \ g \in G$. Then prove that H is a normal sub-gp.

Proof For any $g \in G$, $h \in H$

$gh \in H \Rightarrow (gh)^2 \in H$ and $g^2 \in H$.

Since H is a sub-group

$\therefore h^{-1}g^{-2} \in H$.

So $(gh)^2 h^{-1}g^{-2} \in H$

$\Rightarrow ghghh^{-1}g^{-2} \in H$

$\Rightarrow ghgg^{-2} \in H$

$\Rightarrow ghg^{-1} \in H$

Hence H is a normal sub-gp of G.

Conta

Theorem If p is a prime number, then any group G of order $2p$ has a normal sub-gp of order p

Proof

Since $|G| = 2p$

$2p$ is a composite number with only two divisors 2 & p. ($\because p$ is prime)

$\Rightarrow$ G has only two proper sub-groups

Let the two sub-groups be H & K such that $|H| = 2$ & $|K| = p$

Consider the sub-group K of G

Since $|K| = p$, where p is prime

Therefore K is a cyclic gp of prime order p

Now index of K in $G = [G : K] = \frac{|G|}{|K|}$

$= \frac{2p}{p} = 2$ (by Lagrange's theorem)

Hence K is normal sub-gp of G.

Problem Let A & B be normal sub-gps of a gp G. If $A \cap B = \{e\}$. Then show that $ab = ba$ $\forall\, a \in A$, $\forall\, b \in B$

Solution Suppose that A & B are normal sub-gps of a gp G and $A \cap B = \{e\}$

Let $a \in A$, $b \in B$

Then consider the elements $aba^{-1}b^{-1}$

Then

$aba^{-1}b^{-1} \in A$ $\because$ $ba^{-1}b^{-1} \in A$ & $a \in A$, A being normal

and $aba^{-1}b^{-1} \in B$ $aba^{-1} \in B$, $b^{-1} \in B$, B being normal

$\Rightarrow$ $aba^{-1}b^{-1} \in A \cap B = \{e\}$

So $aba^{-1}b^{-1} = e$

$ab = ba$ (proved)

Theorem If N, A, B are sub-groups of G and $N \Delta A$, then $B \cap N \Delta B \cap A$

Proof Obviously $B \cap N$ & $B \cap A$ are sub-groups of G. Also since $N \Delta A \Rightarrow N \subseteq A$

$\therefore B \cap N \subseteq B \cap A$

So $B \cap N$ is a sub-group of $B \cap A$

Let $u \in B \cap N$ & $v \in B \cap A$

Then $u \in N$ (in particular) & $v \in A$ (in particular)

$\because N \Delta A$

$\Rightarrow v^{-1} u v \in N \quad \forall v \in A, u \in N \longrightarrow (1)$

Again $u \in B$ (in particular) & $v \in B$ (in particular)

Since B is a sub-group of G

$\therefore v^{-1} u v \in B \longrightarrow (2)$

Thus $v^{-1} u v \in B \cap N$ for $u \in B \cap N$ & $v \in B \cap A$

$\Rightarrow B \cap N$ is normal in $B \cap A$

i.e $B \cap N \Delta B \cap A$.

Example Let $Q = \{\pm 1, \pm i, \pm j, \pm k\}$

$H = \{\pm 1, \pm i\}$

Then it is clear that

$aH = Ha \quad \forall a \in Q$. e.g

$\pm j H = \{\pm j \quad \pm k\} = H(\pm j)$

Similarly

$\pm k H = \{\pm j, \pm k\} = H(\pm k)$

Hence H is is normal in Q

Note In fact every subgroup of Q is normal in it

Example: Let $G = \langle a, b : a^3 = b^2 = (ab)^2 = 1 \rangle$ be a group under multiplication and $H = \langle a : a^3 = 1 \rangle$ be a sub-group of G. Show that H is normal in G

Solution: Elements of G are

$1, a, a^2, b, ab, a^2b$ order $= 3 \times 2 = 6$

Now

$1H1^{-1} = H \quad aHa^{-1} = H \quad a^2Ha^{-1} = H$

$H = \{1, a, a^2\}$

$ab\,H(ab)^{-1} = \{ab\,1(ab)^{-1},\ ab\,a(ab)^{-1},\ ab\,a^2(ab)^{-1}\}$

$= \{1,\ ba^2a(ab)^{-1},\ ba^2a^2(ab)^{-1}\}$

$= \{1 \quad bab \quad baab\}$

$= \{1 \quad a^2b^2 \quad ba^2b\}$

$= \{1, \quad a^2 \quad a\} = H$

$b\,H\,b^{-1} = \{1 \quad bab^{-1} \quad ba^2b^{-1}\}$

$= \{1 \quad a^2b\cdot b \quad abb^{-1}\}$

$= \{1 \quad a^2 \quad a\} = H$

$a^2b\,H(a^2b)^{-1} = \{1 \quad a^2ba(a^2b)^{-1} \quad a^2ba^2(a^2b)^{-1}\}$

$= \{1 \quad baa\,b^{-1}\bar{a}^2 \quad ba^3b^{-1}\bar{a}^2\}$

$= \{1 \quad ba^2b^{-1}a^{-2} \quad \bar{a}^2\}$

$= \{1 \quad abb^{-1}\bar{a}^{-2} \quad a\}$

$= \{1 \quad \bar{a}^1 \quad a\} = \{1 \quad a^2 \quad a\} = H$

$b^2 = 1 \quad a^3 = 1$

$\Rightarrow b = b^{-1}, \quad a = \bar{a}^2$

$, a^2 = a^{-1}$

$(ab)^2 = 1$

$\Rightarrow ab = b^{-1}a^{-1}$

$= ba^2$

Similarly

$ba = a^2b$

Hence $gHg^{-1} = H \quad \forall\ g \in G$

$\Rightarrow H$ is normal in G.

End

Example Let M_2 be the group of all 2×2 matrices (singular). Show that

$$S = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix},\ \alpha \neq 0,\ \in R \right\}$$

is normal subgroup of M_2

Solution First we show that S is a subgroup of M_2

For this let $A, B \in S$ Then

$$A = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_1 \end{pmatrix} \qquad B = \begin{pmatrix} \alpha_2 & 0 \\ 0 & \alpha_2 \end{pmatrix}$$

So that $A\bar{B}^1 = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_1 \end{pmatrix} \begin{pmatrix} \frac{1}{\alpha_2} & 0 \\ 0 & \frac{1}{\alpha_2} \end{pmatrix}$

$$= \begin{pmatrix} \alpha_1\alpha_2^{-1} & 0 \\ 0 & \alpha_1\alpha_2^{-1} \end{pmatrix} \in S$$

Hence S is a sub-group of M_2

Next for

$$A = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_1 \end{pmatrix} \text{ in } S$$

and $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in M_2

we have $XAX^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_1 \end{pmatrix}\begin{pmatrix} \frac{d}{D} & -\frac{b}{D} \\ -\frac{c}{D} & \frac{a}{D} \end{pmatrix}$

$$= \begin{pmatrix} a\alpha_1 & b\alpha_1 \\ c\alpha_1 & d\alpha_1 \end{pmatrix}\begin{pmatrix} \frac{d}{D} & -\frac{b}{D} \\ -\frac{c}{D} & \frac{a}{D} \end{pmatrix} \quad \text{where } D = |X| = ad - dc$$

$$= \begin{pmatrix} a\alpha_1\frac{d}{D} - b\alpha_1\frac{c}{D} & -a\alpha_1\frac{b}{D} + b\alpha_1\frac{a}{D} \\ c\alpha_1\frac{d}{D} - d\alpha_1\frac{c}{D} & -c\alpha_1\cdot\frac{b}{D} + d\alpha_1\frac{a}{D} \end{pmatrix}$$

$$= \begin{pmatrix} \alpha_1\left(\frac{ab-bc}{D}\right) & 0 \\ 0 & \alpha_1\left(\frac{ad-bc}{D}\right) \end{pmatrix} = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_1 \end{pmatrix} = A \in S$$

So S is normal in M_2

$$S = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} = \alpha I : 0 \neq \alpha \in R \right\}$$

Smallest normal Sub-gp Containing a Complex

Let M be any complex of G. Then a sub-gp H of G is called smallest normal sub-gp of G containing M if H is normal sub-gp which contains M is contained in every normal sub-gp containing M.

OR

Let M be a complex of G. Then a normal sub-gp H of G containing M is smallest normal sub-gp containing M if H is contained in every other sub-gp containing H.

Theorem The intersection of the family of normal sub-gps which contain a complex is the smallest normal sub-gp containing the complex.

Proof Let $\{H_\alpha, \alpha \in \Omega\}$ be a family of normal sub-gp of a gp G and each H_α contains a complex M.

~~Then as proved earlier $A \in H$~~

Let $H = \bigcap_{\alpha \in \Omega} H_\alpha$

Then as proved earlier H is normal in G.

Also $M \subseteq H$

Let K be any other normal sub-gp containing M. Then K is a member of family $\{H_\alpha : \alpha \in \Omega\}$ and hence

$$H \subseteq K$$

Hence the theorem

Theorem The sub-group generated by the union of M and the complexes conjugate to M is the smallest normal sub-group containing M.

Proof Let H be the sub-gp generated by the union of the complexes of the type

$$x^{-1}Mx \qquad x \in G$$

is normal

Every element a of H is expressible as

$$a = b_1 b_2 \text{---} b_i$$

where each b_i is either a member of complex of the form $x^{-1}Mx$ for some x or inverse of some element of the same type.

Now

$$y^{-1}ay = y^{-1}b_1 b_2 \text{---} b_i\, y$$

$$= y^{-1}b_1 y y^{-1} b_2 y y^{-1} \cdot b_3 \text{---} b_{i-1}\, y y^{-1} b_i y$$

$$= (y^{-1}b_1 y)(y^{-1}b_2 y)(y^{-1}b_3 y) \text{------} (y^{-1}b_i y)$$

$\Rightarrow y^{-1}ay \in H$.

Thus H is normal

Also every normal sub-group K containing the complex M must necessarily contain complex $x^{-1}Mx$ conjugate to M

$\Rightarrow K \supseteq H$, H being union of complexes of type $x^{-1}Mx$.

Factor Group or Quotient Group or Facl

Let G be a group and H be a normal subgp of G. Consider the set

$$\Theta = \{aH : a \in G\} = \{Ha : a \in G\}$$

of all right cosets of H in G.

Now we show that Θ is a group

(i) Define a multiplication in as follows

For $aH, bH \in \Theta$ we put

$$aH \cdot bH = abH$$

We show that this multiplication is well defined (i.e does not depends on the choice of representatives a & b but depends on the cosets aH & bH themselves)

For this let $ah \in aH$ $bh' \in bH$

Then

$$\begin{aligned}(ah)H \cdot (bh')H &= (ah)(bh')H \\ &= a(hbh')H \quad \text{(Ass. Law)} \\ &= a(bh_1h')H \quad \because H \triangle G \\ &= (ab)(h_1h')H \quad \therefore b^{-1}hb \in H \\ &= (ab)H \quad \Rightarrow b^{-1}hb = h_1 \in H \\ &\quad \because h_1h' \in H \quad \Rightarrow hb = bh_1\end{aligned}$$

$\Rightarrow$ multiplication is well defined.

OR

Let $aH = a_1H$, $bH = b_1H$

Then we have to show that $abH = a_1b_1H$

Since $aH = a_1H$ $bH = b_1H$

$\Rightarrow a_1 = ah_1$ $b_1 = bh_2$ for some h_1, h_2

$$\Rightarrow a_1b_1 = (ah_1)(bh_2) = a(bb^{-1})h_1bh_2 = (ab)\,b^{-1}h_1(b^{-1})^{-1}h_2$$

$\because H$ is normal

$\Rightarrow b^{-1}h_1(b^{-1})^{-1} \in H$

Consequently $b^{-1}h_1(b^{-1})^{-1}h_2 \in H$ & $b^{-1}h_1(b^{-1})^{-1}$

Then $a_1b_1H = (ab)(b^{-1}h_1(b^{-1})^{-1}h_2)H$

$= abH$

This proves that the binary composition is well defined.

(ii) Associative Law

Let $aH, bH, cH \in Q$. Then

$(aH \cdot bH)(cH) = (ab)H \cdot (cH) = ((ab)c)H$

$= (aH)((bc)H)$

$= aH(bH \cdot cH)$

So $(aH \cdot bH)(cH) = aH(bH \cdot cH)$

Hence associative Law is satisfied in Q

(iii) Existence of Identity

The coset $eH = H$

is the identity element of Q. Here for any $aH \in Q$

$aH \cdot eH = (ae)H = aH$

(iv) Existence of Inverse

For any $aH \in Q$, $a \in G$, $a^{-1}H \in Q$ and

$(aH)(a^{-1}H) = (aa^{-1})H = eH = H$

Hence $a^{-1}H$ is an inverse of aH i.e.

$(aH)^{-1} = a^{-1}H$

Hence Q is a group. The group Q is called the Quotient group or factor group of G by H and is denoted by G/H.

Defination: The group formed of the set of all cosets of a normal sub-group H of a gp G together with (binary) multiplication of complexes as composition is called the Quotient group of G relative to H (or by H) and is denoted by G/H (read as "G over H or 'G factor H or the factor gp of G by H)

Remarks • Since $gH = Hg$ for normal sub-gp H, therefore we donot have to distinguish between the right and the left cosets of decomposition of H

• Apparently it looks that the product

$(aH)(bH)$ depends on the choice of the representatives a and b of aH & bH. However if define the product of two cosets, we will like that this product should depend on the cosets aH & bH themselves but not on a, b because it is conceivable that if $aH = a_1H$, $bH = b_1H$ but $abH \neq a_1b_1H$. In such case what should we take for the product of two cosets, abH or a_1b_1H. Hence we must show that the product of two cosets is uniquely defined by the formula $(aH)(bH) = abH$ i.e if $aH = a_1H$, $bH = b_1H$ then $aa_1H = bb_1H$

Example Let Z be the group of integers under addition. Let $H_3 = \{3k : k \in Z\}$

Then H_3 is a normal subgroup of Z

The distinct cosets of H_3 in Z are.

$\bar{0} = 0 + H_3 = H_3$ $\quad$ $\bar{1} = 1 + H_3$

$\bar{2} = 2 + H_3 =$ etc $\quad$ $\bar{3} = 3 + H_3 = 0 + H_3 = \bar{0}$

$\bar{4} = 4 + H_3 = 1 + H_3 = \bar{1}$

So $Z/H_3 = \{\bar{0}, \bar{1}, \bar{2}\}$ is the quotient or factor group of Z by H_3

The addition table of Z/H_3 is

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

Similarly Let $Hn = \{kn : k \in Z\}$

The distinct Cosets of H_3 in Z are

$\bar{0} = 0 + Hn = Hn$

$\bar{1} = 1 + Hn =$

$\bar{2} = 2 + Hn$

$\overline{n-1} = (n-1) + Hn$

So $Z/Hn = \{\bar{0}, \bar{1}, \bar{2}, \ldots\ldots \overline{n-1}\}$ is group under the addition defined

$$a + Hn + b + Hn = r + Hn$$

where r is remainder obtained after dividing the usual sum of a, b by n. This group is factor group of Z by Hn.

Addition table for Z/Hn is

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	- - - - -	$\overline{n-1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	- - - - -	$\overline{n-1}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	- - - - -	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	- - - - -	$\bar{1}$
⋮	⋮	⋮	⋮	⋮	⋮
$\overline{n-1}$	$\overline{n-1}$	$\bar{0}$	$\bar{1}$		$\bar{0}$

Example Let $Q = \{\pm I, \pm i, \pm j, \pm k\}$ be the group of quaternions under multiplication and $H = \{\pm I\}$

Then H is normal in Q. The distinct cosets of H in Q are

$$IH = H \quad \text{or} \quad -IH = H$$
$$iH, \; jH, \; kH$$

So $Q/H = \{H, iH, jH, kH\}$

The multiplication table is

·	H	iH	jH	kH
H	H	iH	jH	kH
iH	iH	H	kH	jH
jH	jH	kH	H	iH
kH	kH	jH	iH	H

$iH \cdot iH$
$= i^2H = -1H = H$

Note order of each coset is 2 & order of G/H is 4

Theorem: Quotient group of an abelian gp is abelian.

Proof: Let G be an abelian gp and H be its normal subgroup.

Let $aH, bH \in G/H$, where $a, b \in G$

$(aH)\cdot(bH) = (ab)H$
$= (ba)H$
$= (bH)\cdot(aH)$

$\therefore G/H$ is abelian

Theorem Every quotient group of a cyclic group is cyclic

Proof Let G be a cyclic group and $a \in G$ be the generator. Let H be normal sub-group of G.

Now $a^n \in G$ where n is some integer

Also $a^nH \in G/H$

But $a^nH = (a\cdot a\cdot a \text{ ---- } n \text{ times})H$
$= (aH)(aH) \text{ ---- } n \text{ times}$
$= (aH)^n$

As n varies, (a) gives all elements of G and consequently $(aH)^n$ gives all elements (cosets) in G/H. Hence (aH) is the generator of G/H. Therefore G/H is cyclic.

(Qazi-85)

Problem N is a normal subgroup of a group G. Show that G/N is abelian if and only if for all $x, y \in G$, $xyx^{-1}y^{-1} \in N$.

Solution:

Let $xyx^{-1}y^{-1} \in N \quad \forall x, y \in G$

$\Rightarrow xyx^{-1}y^{-1}N = N$

$\Rightarrow xNyN(xN)^{-1}(yN)^{-1} = N$

$\Rightarrow xNyN = (yN)xN$

$\Rightarrow G/N$ is abelian

Conversely let G/N is abelian, then for $x, y \in G$

$xNyN(xN)^{-1}(yN)^{-1} = (xN)(xN)^{-1}(yN)(yN)^{-1} = NN = N$

Now

$xyx^{-1}y^{-1}N = xNyNx^{-1}Ny^{-1}N = xNyN(xN)^{-1}(yN)^{-1} = N$

$\Rightarrow xyx^{-1}y^{-1} \in N$.

(Qazi-85)

Problem:- If G is a group such that $G/Z(G)$ is cyclic, where $Z(G)$ is the centre of G. Show that G is Abelian.

Solution

Put $N = Z(G)$ and let $G/N = \langle gN \rangle$ for some $g \in G$

Let $a, b \in G$, then

$aN = (gN)^k = g^kN$

and $bN = (gN)^l = g^lN$ for some $k, l \in Z$

Thus $a = g^k n_1$ and $b = g^l n_2$, $n_1, n_2 \in N$

$\Rightarrow ab = g^{k+l} n_1 n_2$ & $ba = g^{l+k} n_1 n_2$ as $n_1 n_2 \in N = Z(G)$

Hence $ab = ba$

demanded by Group $(G, *)$ is called Commutative gp. if the following is remarks.

demanded by This no

dem

Fr.st Thod

This no not denounced by

egu equal

d

سینٹ جارجس

ٹیڈول لمب

گلہ بارش اِنا کھتروے رہ وچوں مرپانے
کھڑے رکھوں رہ تے آسن کم ہمبا ے

اپنا آپ سنگھار کھیدا دل نئیں آکھدا
سر مڑھے لئے کھوں مسجد سے نہ چھوٹے بعیدل والے

ہمدرد.

بارش اِتنا کھبوے وسیہہ لوکاں پیرنائے
کھڑے رکھوں لاتے آسن کم ہُنا ے

آپنا آپ سنگھار کھیدا دل نئیں آکھدا
رکھیں سکیں تے گوں مسجد سے نئیں چھوٹے بعیداں والے

لنڈی کی کوئی ذرا ایکلم — البرٹ ریناؤ
ہمدرد — سنز رودیلن نہ نہ نائیلن سن

Matt

packet of statistical programs

Statagraphic. Reg 15.